サイバネティック・アバターにおけるリスクとセキュリティ要件の整理

加藤 大弥[1,a)]　津田 侑[3]　砂原 秀樹[2]　佐藤 雅明[1]

概要：人の身体的能力、認知能力及び知覚能力を拡張する ICT 技術やロボット技術を含む概念であるサイバネティック・アバター（CA）を実現するための基盤技術として、身体能力・認知能力・知覚能力をデータとして伝送する経路をデジタル神経と提唱している。このデジタル神経を構成する技術は、その特性上、従来のインターネット通信やロボット制御とは異なる性能や安全性が求められる。そこで本研究では、この CA とデジタル神経という概念におけるセキュリティ、すなわち CA セキュリティの重要性について論じ、既存のデジタル空間におけるセキュリティとの相違点や、CA 特有の要件とリスクを整理する。これにより、CA 社会における新たなセキュリティ領域の議論を提示する。

キーワード：セキュリティ, CA セキュリティ, サイバネティック・アバター, VR, CPS

Systematization of Risks and Security Requirements in Cybernetic Avatar

Daiya Kato[1,a)]　Yu Tsuda[3]　Hideki Sunahara[2]　Masaaki Sato[1]

Abstract: The Cybernetic Avatar (CA) concept, which encompasses ICT and robotic technologies to enhance human physical, cognitive, and perceptual abilities, relies on a fundamental technology for transmitting these capabilities as data. In our current work, we refer to this transmission pathway as a Digital Nervous System. Due to its nature, the technologies comprising this Digital Nervous System require performance and security considerations that differ from conventional Internet communications and robotic control systems. This study focuses on the security aspects of the CA and its Digital Nervous System—collectively referred to here as CA security—and outlines how they differ from existing security in digital environments. We organize CA-specific requirements and risks to highlight emerging issues that need to be addressed for the secure realization of a future CA society.

Keywords: Security, CA security, Cybernetic Avatar, VR, CPS

1. はじめに

サイバネティック・アバター（Cybernetic Avatar: CA）は、人間の身体的能力、認知能力、知覚能力を拡張し、他者や環境と新たなかたちで関わることを可能にする次世代 ICT・ロボット技術の統合概念である。従来のロボット遠隔操作や VR/AR 技術は、主に視覚・聴覚情報の提示や動作の遠隔実行に重点を置いてきた一方で、CA は五感情報や精緻な動作データなど、人間の主体的な行為と体験をインターネットを介して伝送し、あたかも自らの身体であるかのようにアバターを感じながら行動できる点に特徴がある。これにより操作者が自身の身体的特徴や距離に縛られることなく、主体感・身体所有感の付与されているアバターを操作することにより広く社会に参画でき、人間を中心とした身体的共創を目的としている。

この身体的共創を生み出すサイバネティック・アバター技術と社会基盤を実現にあたり、CA の社会実装における

[1] 東海大学 Tokai University
[2] 慶應義塾大学 Keio University
[3] Turnt Up Technologies 株式会社 Turnt Up Technologies, Inc.
[a)] daiya@tokai.ac.jp

倫理・制度的課題への配慮とともに、安全・安心を支えるセキュリティ基盤の確立が不可欠である。特に、CA の実現を支える身体的能力・認知能力・知覚能力をデータとして伝送する経路 (本研究ではこれをデジタル神経と呼ぶ) は、その特性上、従来のインターネット通信や産業用ロボット制御とは異なる性能要件や脅威モデルを持つ。これには、リアルタイム性と高信頼性に加え、利用者の身体的安全、プライバシー、倫理的整合性を確保する新たなセキュリティ要件が求められる。

そこで本研究では、CA とデジタル神経という概念におけるセキュリティ、すなわち CA セキュリティの重要性を議論する。既存のサイバーフィジカルシステムや VR/AR、遠隔ロボット制御のセキュリティとの差異を明らかにするとともに、CA 特有の利用シナリオや社会的要請から導かれる要件・リスクを整理し、今後の CA 社会における新たなセキュリティ領域の議論を提示することを目的とする。

本稿の構成は以下の通りである。2 節では CA の定義やこれまでの取り組み、ユースケースを整理して説明する。3 節では CA と類似要素がある領域のセキュリティの先行研究について述べる。これらを踏まえて、4 節では CA 独自の特徴を組み込んだ CA セキュリティについて議論する。最後に、5 節と 6 節で今後の課題とまとめを述べる。

2. サイバネティック・アバター

2.1 CA の定義

サイバネテック・アバターの定義は、「サイバネティック・アバターは、身代わりとしてのロボットや 3D 映像等を示すアバターに加えて、人の身体的能力、認知能力及び知覚能力を拡張する ICT 技術やロボット技術を含む概念。」[1][2][3] である。CA はあくまでも人の身体的能力、認知能力及び知覚能力を拡張することが目標であるため、ユースケースとして AI の活用や自動化による完全自律的なロボットではなく、人間の意思として動作するということが重要である。

2.2 CA 社会実現に向けた取り組み

CA 社会実現に向けた取り組みの一例を示す。分身ロボットカフェ DAWN ver. β [4] では、外出困難者が分身ロボット OriHime–D を遠隔操作し、接客業務を通じて社会参画を果たす取り組みが進められている。また、MWC2024 において NTT ドコモ、慶應義塾大学は、5G/IOWN ネットワークを活用してアバターの高精度制御と触覚伝送を実現する FEELTECH を発表し、基盤技術である FEELTECH Wear[5] による触覚体験の観光案内や現場作業支援など多様な応用可能性を提示している [6]。実際の主体感のある体験共有の取り組みとしては、Zhu らの陶芸における暗黙知の技能伝達を目的として、触覚や運動データを記録・再現する研究 [7] や、佐藤らの二腕型ロボティックアバターを多人数で協調操作することで複数の操作者が一体のアバターを身体統合的に制御する取り組み [8] についても進められている。

このように技能や経験がネットワークを介して流通し、人間の身体的・認知的・知覚的能力を拡張し、地理的・身体的制約を超えて活動できる社会、CA 社会 [1][9] の実現を目指している。

2.3 CA のユースケース

CA を介した基本的なユースケースを図 1 に示す。この図では操作者がヘッドマウントディスプレイを装着し、何らかの方法で遠隔から CA を操作することで対象者とコミュニケーションをとっている。例えば対象者と握手をする場合、操作者が握手をするという意思を CA に操作として反映させ、速やかに CA に反映され対象者と握手を実行することで、あたかも操作者が見ている視覚情報では主体感を持って対象者と握手をすることを可能にする。この際、視覚情報でなく操作者の手に対して触覚等のフィードバックを返すことで、より主体感のある体験を得ることが可能である。

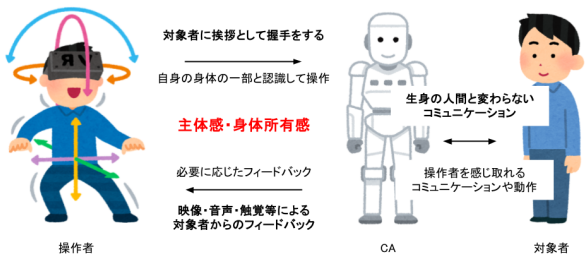

図 1 CA を介した基本的なユースケース

応用的なユースケースとしては、1 つの CA に対して複数の操作者がいる例を図 2 に示す。この図では操作者 A、B が共同で陶芸を行う例である。素人と玄人の操作に重みをつけて CA に反映することで、素人は玄人の能力が反映された状態、つまり自身の能力が拡張された状態の体験を主体感を持って得ることが可能である [8]。これにより素人は自身の能力を拡張して行動ができるだけではなく、操作者の効率的なスキルアップにもつながることが期待される [7]。

2.4 操作形態、CA の分類

これらのユースケースや宮下らの研究 [10] から CA の分類について示す。まず操作形態については、以下の 4 つに分類される。

単一操作者–単一アバター

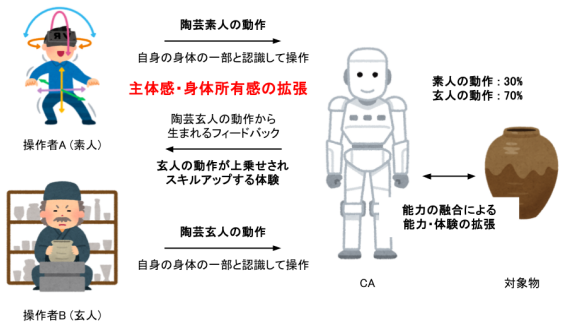

図 2　CA を介した応用的なユースケース

基本的な 1 対 1 の操作

単一操作者–複数アバター

1 人の操作者が複数のアバターを同時または切り替えて操作

複数操作者–単一アバター

複数人で 1 つのアバターを協調操作

複数操作者–複数アバター

複数人で複数のアバターを同時または切り替えて操作

次にアバターの種類については表 1 のように、物理アバター、バーチャルアバター、複合アバターの 3 種類に分類される。

このように操作形態と CA の種類を組み合わせることで身体的制約や地理的制約を越えて多様な人々が社会活動に参加するための、物理空間とデジタル空間両方での活動のスケーラビリティ・インターオペラビリティを実現している。

3. 先行研究

以上に挙げた CA に関するセキュリティの包括的議論は現時点ではほとんど存在しない。したがって本研究では CA と類似する要素を有する既存領域である、VR/AR 環境、サイバーフィジカルシステム（CPS）におけるセキュリティ研究を参照しつつ、CA セキュリティを議論する。

VR/AR 環境におけるセキュリティについては、金岡ら [11] が脅威と攻撃対象領域の体系的分析を行っており、情報漏洩、なりすまし、環境改ざん、感覚情報の偽装など、多様な攻撃手法と防御策が整理されている。これらの知見は、CA における視覚・聴覚情報や空間情報の保護に直接応用可能である。しかし、VR/AR 研究の多くは物理世界との直接的接触や物体操作を前提としていないため、CA の特徴である物理的インタラクションや実環境への作用に伴う安全性・信頼性の課題は十分に議論されていない。

一方、CPS や産業分野におけるセキュリティ研究では、STRIDE モデル [12] を応用した脅威分析手法が広く用いられている。例えば、Khan ら [13] はスマートグリッド等の CPS において、改ざんや拒否、権限昇格、サービス拒否といった攻撃を体系的にモデル化している。また、Industrie 4.0 における設計原則 [14] や、人間中心の製造産業を志向する Industry 5.0 の技術ロードマップ [15]、および協働ロボットのセキュリティ課題 [16] では、実世界に作用するシステムの安全性確保や人と機械の協調作業におけるリスク低減が重視されている。さらに、自動運転車両 [17] や協働ロボット [18] の研究では、低遅延制御やセンサー情報の信頼性保証が求められることが示されている。これらは CA の物理的制御や環境作用に関する脅威モデル構築の参考となるが、操作者が主体的に遠隔から身体を拡張するという CA 特有の体験設計までは考慮していない。

CA に関連する既存のセキュリティの議論として、先に述べた Sato らの研究 [8] では、操作者間の同期制御や役割分担といった協調操作に伴う制約や技術的課題が報告されている。また、宮下らによる CA プラットフォーム [10] では、セキュリティに関しては明確な言及は行われていないが、操作者認証や利用権限管理、通信経路 (WebRTC, WebSocket) の低遅延・高信頼性確保の必要性について示されている。その中でも新保らによる CA における認証や法的解釈等の社会的セキュリティ課題の議論 [19] についても進められている。

4. CA セキュリティ

以上より本研究では、CA 独自の特徴を体系的に組み込んだセキュリティである、CA セキュリティについて議論を行う。

4.1 CA セキュリティの定義

本研究で議論する CA セキュリティは、「サイバネティック・アバターを主体感と身体所有感を伴って制御する一連の過程において、操作者・対象者の安全性・プライバシー・信頼性・倫理的整合性を保証し、かつシステム全体の継続的な可用性を維持するためのセキュリティ技術・運用」と定義する。

4.2 CA セキュリティの特徴

CA セキュリティでは、既存のサイバーセキュリティが対象としてきた情報の機密性・完全性・可用性に加えて、CA 特有の身体性・主体性を保護する必要があることが大きな特徴である。CA は操作者が主体感や身体所有感を持った状態で遠隔地や仮想空間に作用するため、従来の情報システムやサイバーフィジカルシステムとは異なるリスク構造を持つ。

具体的には、物理世界での接触や作業を伴うため身体的安全性が必須であり、さらに操作者や対象者の行動・発言・反応といったインタラクションが心理的・精神的な影響を及ぼす可能性がある。また、映像・音声・触覚・力覚・動作等の多様なモダリティ情報がリアルタイムで双方向に伝

表 1　アバターの種類

種類	説明	特徴	例
物理アバター	遠隔操作ロボットなど、物理世界で直接作用するアバター	物理的インタラクション (物体操作、移動、接触) に対応し、作業支援や接客などに利用可能	二腕型作業ロボット、移動型ロボット
バーチャルアバター	CG キャラクターや 3D モデルとしてデジタル空間に存在するアバター	物理的制約がなく、表現やデザインの自由度が高い。教育、会議、イベントなどで活用可能	デジタル空間内のアバター、メタバース上のキャラクター
複合アバター	物理アバターとバーチャルアバターの両方の特徴を併せ持つアバター	物理とデジタル空間をまたぐ活動が可能で、情報提示や操作方法の柔軟性が高い	物理ロボットの動きが同時にデジタル空間のアバターにも反映されるシステム

送されるため、情報の漏洩・改ざん・不正利用のリスクが増大する。加えて、単一操作者–複数アバターや複数操作者–単一アバター等の多様な操作形態では、権限管理や同期制御の複雑化、メーカーやプラットフォーム間のインターオペラビリティに伴う課題が顕著になる。

4.3　CA セキュリティの対象

CA セキュリティの対象について図 3 示す。CA の制御の一連の過程における対象を以下の通り 5 つに分類する。

- 操作者
  - CA を操作する人
  - 特徴: 多様な国籍・人種・言語・文化・身体的等の背景を有する人間
- CA
  - 操作者が操作するサイバネティック・アバター
  - 特徴: 物理、デジタルに関係なく、様々な形・機能・能力を持つアバター。人間を超えた能力も出力可
- 対象者
  - CA がインタラクションを起こす対象
  - 特徴: 多様な国籍・人種・言語・文化的・身体的等の背景を有する人間。また多様な物体
- デジタル神経
  - 操作者と CA を繋ぐデータの伝送路。本研究ではデジタル神経と呼称
  - 特徴: ネットワークを介した操作者–CA 間のデータの伝送
- インタラクション
  - CA と対象者で発生するインタラクション
  - 特徴: 物理・言語・精神・心理的等の動作やコミュニケーション

4.4　CA セキュリティの主要脅威カテゴリ

CA における脅威は多岐にわたるが、本研究では後続の攻撃分析や防御設計の基盤とするため、これらを大きく 5 つの脅威カテゴリに分類する。この分類は、実際の脅威事例や攻撃手法を体系的に整理する際の脅威カテゴリとして機能し、各カテゴリの下により具体的なリスクやシナリオ

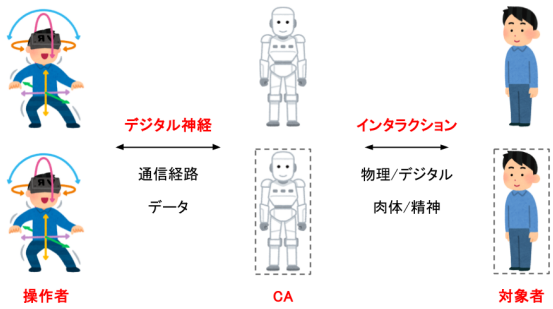

図 3　CA セキュリティの対象

を位置づけることができる。

物理的影響を伴う脅威

操作者が操作する CA の誤操作や不正操作、制御信号の改ざんによる衝突・転倒・接触など、身体的危害をもたらす事象。

心理的・精神的影響を伴う脅威

対象者が CA を単なる機械として扱い、暴言・破壊・侮辱等の行為を行うことで、操作者が精神的損害を被る事象。

多様なモダリティ情報に対する脅威

映像・音声に加え、触覚、力覚、動作データなど高精度でセンシティブな情報が伝送されるため、その盗聴・改ざん・不正利用によるリスクが高い。

多人数・多拠点操作の複雑性

単一操作者–複数アバターや複数操作者–単一アバターなど、多様な操作形態が存在し、権限分配や同期制御が複雑化する。

CA のインターオペラビリティ

メーカーや仕様の異なる CA の接続インタフェースやプロトコルが新たな脆弱性の温床となり得る。

4.5　CA 社会における攻撃

4.5.1　目的と脅威アクター

CA 社会における攻撃の目的と脅威アクターは、既存のサイバー攻撃における目的 [20] および脅威アクター [21] に加え、CA 独自の特徴を利用した新たな形態が想定される。

表 1 に示すように、物理アバター・バーチャルアバター・複合アバターの種類ごとに、その特性に応じて攻撃目的や脅威アクターが異なる。

物理アバターを利用した攻撃では、対象者に対して直接的な身体的被害や物理的抑止を与えることが主要な目的となり得る。そのため、強い動機を有するハクティビストやテロリストが脅威アクターとして想定される。また、CA が距離や身体的制約を超えて活動できる特性を悪用し、諜報活動を目的とする攻撃も考えられる。

バーチャルアバターの場合、物理的制約が存在しないため、広範な表現や組織的活動を通じた攻撃が可能となる。その結果、強固な組織力や統制力を背景に、デジタル空間における影響力拡大を目的とするカリスマ的なハクティビストが脅威アクターとして想定される。

複合アバターは、物理空間とデジタル空間をまたぐ活動を可能にするため、上記両者で想定される脅威アクターが共通して現れる。ただし、現時点における複合アバターの社会的ユースケースは限定的であり、その具体的な攻撃目的やシナリオは十分に整理されていない。

さらに、CA 特有の攻撃として、操作者になりすまして攻撃を実行し、その責任を正規操作者に押し付ける手法が挙げられる。このような攻撃は、操作者の社会的信用を損なわせ、意図せぬ加害者として責任や法的制裁を負わせる可能性がある。その影響範囲は、従来のサイバー攻撃における情報資産への被害にとどまらず、物理空間や操作者本人、さらには対象者にまで広がる点で特徴的である。

4.5.2 アタックサーフェス

CA 社会におけるアタックサーフェスは、図 3 で示した各要素を包含し、従来の情報システムにおけるサーバやネットワーク境界のみならず、操作者の身体性や主体性にまで拡張される点に大きな特徴がある。操作者の入力インタフェースについては、先行研究 [11] においても議論されているように、ヘッドマウントディスプレイ、ハプティックデバイス等のアクチュエータ全般が攻撃対象となり得る。操作者と CA を接続するデジタル神経については、目的や利用文脈が異なるものの、ネットワーク通信に対する従来型のアタックサーフェス（盗聴、改ざん、サービス拒否等）が想定される。

CA そのものに関しては、物理アバターやバーチャルアバターに加えて、それらの稼働に必要な充電ステーションや関連機器などのサイドチャネルも攻撃対象となる。対象者とのインタラクションにおいては、物理的接触、音声会話、視覚的フィードバックといった双方向のコミュニケーションそのものがアタックサーフェスとして機能し得る。特に、対象者自身が CA を介して操作者に対して肉体的あるいは精神的な影響を与える場合には、CA 特有の新たな攻撃経路が生じる。

さらに、CA 社会を担う CA 関連サービスが誕生する際、これらも主要なアタックサーフェスとして位置付けられる。これら多様なアタックサーフェスは複合的かつ人間の肉体・精神に直接作用するため、従来の IT システムに比べてより高度で統合的なアタックサーフェスマネジメントが不可欠となる。

4.5.3 攻撃手法

CA に対する攻撃手法は、その多様性において既存のサイバー攻撃と本質的に共通する部分が多い。すなわち、攻撃の目的やアタックサーフェスに応じて、既存の情報システムで確認されている盗聴、改ざん、リプレイ攻撃、サービス拒否攻撃などの多様な手法が適用可能である。しかし、CA はロボティクス技術および人間の身体性・主体性を含む複合的なシステムであるため、攻撃手法も従来の範疇を超えて拡張される。

具体的には、通信経路（デジタル神経）に対する攻撃として、従来型の盗聴や改ざんに加え、操作者が取得する視覚・聴覚・触覚情報そのものを改ざんする感覚のハイジャックが想定される。この場合、操作者の主体感や身体所有感が直接的に侵害され、心理的混乱や誤操作を誘発する可能性がある。また、CA 特有の攻撃として、操作者のなりすましが重大な脅威となる。認証情報を乗っ取ることで CA を不正操作するだけでなく、多人数操作環境においては妨害行為や協調性の破壊を引き起こすことも可能である。

さらに、物理アバターに対しては、既存のロボティクス分野で議論されているように、破壊工作や違法改造、ファームウェアへの不正な書き換えなどの攻撃が統合的に考慮される必要がある。これらは直接的な物理的危害や長期的な信頼性低下につながるため、CA 社会特有のリスクとして位置付けられる。

4.6 CA 社会における防御

4.6.1 脅威分析

CA 社会における攻撃は、従来の情報システムに比べてより広範囲に影響が及ぶため、脅威分析もそれに応じた拡張が必要となる。基本的な方針としては、先行研究 [11] でも整理されているように、既存の STRIDE モデル [12] を基盤として適用することを想定しているが、その適用範囲や各項目の内容は CA 特有の特徴に即して再定義される必要がある。具体的な例を示す。

Spoofing（なりすまし）
: 操作者認証の乗っ取りによる不正操作や、アバター自体の偽装によって対象者を欺く攻撃。

Tampering（改ざん）
: 操作者から CA に送信される動作制御信号、あるいは触覚・力覚といった感覚データの改ざんによる誤操作や錯覚の誘発。

Repudiation（否認）
多人数操作環境における操作ログの欠如や不完全性による、責任追跡や証跡管理の困難化。

Information Disclosure（情報漏洩）
映像・音声に加えて、触覚や動作パターンといった多様なモダリティ情報の不正取得によるプライバシー侵害。

Denial of Service（サービス拒否）
低遅延性が求められるデジタル神経通信を標的とした遅延注入や遮断、さらにはインタラクションの強制停止。

Elevation of Privilege（権限昇格）
複数操作者環境における不正な権限取得、優先度操作や制御権限の独占。

さらに STRIDE を CA に適用する場合、CA 特有の操作者や対象者といった人間そのものへの身体的・心理的脅威については当然考慮されていない。そこで以下のような CA セキュリティ特有の脅威を追加の分析項目として拡張的に取り入れることが必要である。

Physical Harm（身体的被害）
CA の誤操作や不正制御、通信遅延により操作者や対象者が転倒・衝突・挟まれといった身体的危害を受ける可能性。

Psychological Harm（心理的・精神的被害）
対象者や他操作者からの暴言・ハラスメント行為、または偽装された感覚情報の提示により、操作者が心理的ストレスやトラウマを負う可能性。

Social Trust Harm（社会的信用の毀損）
操作者になりすました CA の行動が第三者に被害を与え、正規操作者の社会的評価や信用を損なう可能性。

4.6.2 リスク分析

リスク分析の枠組みとしては、TVRA（Threat, Vulnerability, and Risk Analysis）の応用が有効であると考えられる。TVRA は、潜在的脅威（Threat）、システムが有する既知・未知の脆弱性（Vulnerability）、およびそれらが結びついた場合に生じるリスク（Risk）を体系的に整理し、発生可能性と影響度の両面から評価する柔軟な手法である。

CA 社会において TVRA を適用する場合、図 3 で示した操作者、CA、対象者、デジタル神経、インタラクションといった多様なアタックサーフェスに対して、潜在的脅威と脆弱性を対応づけることで、CA 特有のリスクマップを構築することが可能となる。例えば、デジタル神経における低遅延通信は DoS 攻撃に対して脆弱であり、操作者認証の不備はなりすまし攻撃に直結するなど、アタックサーフェスごとのリスクの具体化が必要である。

4.6.3 防御手法

CA セキュリティにおける防御設計は、前節で示した脅威カテゴリを基盤として検討される。防御手法は従来の情報システムにおける対策を踏襲しつつも、CA 特有の身体性・主体性・多様なモダリティ性を考慮した拡張が必要となる。ここでは、各脅威カテゴリに対応する技術的対策と制度的・運用的対策を想定例として整理する。表 2 に、各脅威カテゴリに対応する想定される防御手法を示す。

5. 今後の課題

本研究では CA セキュリティにおける脅威カテゴリや防御手法を整理したが、これらはあくまで現状までの知見と想定に基づくものであり、実際の CA 社会でどのように機能するかの検証は不十分である。今後は本研究で示した分類を実際のユースケースに適用し、検証・評価を通じて不足している点を補い、最終的にはフレームワークやガイドラインとして体系化していく必要がある。

特に、より詳細なリスク分析手法として TVRA を CA に適用し、各アタックサーフェスに対する潜在的脅威、脆弱性、発生可能性、影響度を組み合わせたリスクマップを構築することが重要となる。そのためには、CA や社会環境を実際に利用した実験的検証を進め、想定された攻撃手法や防御策の実効性を確認していくことが求められる。

また、CA セキュリティにおいて特徴的なのは、操作者や対象者の身体的安全や心理的・精神的影響といった定量化が困難な要素を含む点である。これらは従来の情報システムのリスク評価では十分に扱われてこなかった領域であり、発生頻度や影響度の評価指標自体の拡張が必要である。したがって、TVRA を基盤としつつも、人間中心の安全性・信頼性を組み込んだ新たなリスク分析枠組みの設計が今後の重要な課題である。

6. まとめ

本研究では、人の身体的能力、認知能力、知覚能力を拡張するサイバネティック・アバター（CA）の社会実装に不可欠な要素として、CA セキュリティについて検討した。CA セキュリティを「サイバネティック・アバターを主体感と身体所有感を伴って制御する一連の過程において、操作者・対象者の安全性・プライバシー・信頼性・倫理的整合性を保証し、かつシステム全体の継続的な可用性を維持するためのセキュリティ技術・運用」と定義し、その上で、現状の知見から今後の CA セキュリティを考えていくための基礎基盤として、CA 特有のリスク要因を抽出し、物理的影響、心理的・精神的影響、多様なモダリティ情報、複数操作者・複数アバター環境、インターオペラビリティといった主要な脅威カテゴリを提示した。また、CA 社会における攻撃の目的、脅威アクター、アタックサーフェスを分析し、既存の STRIDE モデルを拡張して身体的・心理的被害を新たな分析項目として取り込む必要性を示した。加

表 2　CA セキュリティにおける主要脅威カテゴリと想定される防御手法の例

脅威カテゴリ	技術的対策（想定例）	制度的・運用的対策（想定例）
物理的影響を伴う脅威	・フェイルセーフ設計 ・衝突回避アルゴリズム ・異常検知による制御停止	・安全規格に基づくルール ・操作者教育・訓練 ・リスクアセスメント
心理的・精神的影響を伴う脅威	・暴言・嫌がらせ検知 ・不適切行為検出	・モデレーション方針 ・倫理ガイドライン ・ハラスメント対応
多様なモダリティ情報に対する脅威	・エンドツーエンド暗号化 ・リプレイ攻撃対策 ・改ざん検知	・データ保護規制 ・利用ポリシーの明示 ・監査ログ追跡
多人数・多拠点操作の複雑性	・多要素認証 ・権限分離 ・同期制御検証	・権限管理ポリシー ・責任分担
インターオペラビリティに伴う脅威	・API/プロトコル標準化 ・相互接続テスト ・脆弱性検証	・第三者評価制度 ・セキュリティガイドライン

えて、防御手法の検討においては、技術的対策と制度的・運用的対策を組み合わせた包括的アプローチが重要であることを整理した。

以上の整理により、CA セキュリティは従来の情報システムセキュリティの延長では捉えきれない新たな領域であることを明確にした。本研究の成果は、CA 技術の社会実装に向けたセキュリティ研究の出発点として基盤的知見を提供するものである。

謝辞　本研究は JST ムーンショット型研究開発事業「身体的共創を生み出すサイバネティック・アバター技術と社会基盤の開発」（Grant number JPMJMS2013）の一環として実施されました。

参考文献

[1] ムーンショット目標 1　2050 年までに、人が身体、脳、空間、時間の制約から解放された社会を実現. https://www8.cao.go.jp/cstp/moonshot/sub1.html.

[2] Norihiro Hagita, Ryota Kanai, Hiroshi Ishiguro, Kouta Minamizawa, Fumihito Arai, Fumio Shimpo, Takeshi Matsumura, and Yoko Yamanishi. Cybernetic avatars: Teleoperation technologies from in-body monitoring to social interaction. *Science Robotics*, Vol. 9, No. 96, p. eadg1842, 2024.

[3] Hiroshi Ishiguro. *Introduction: Cybernetic Avatar*, pp. 1–9. Springer Nature Singapore, Singapore, 2025.

[4] 分身ロボットカフェ DAWN ver. β. https://dawn2021.orylab.com/.

[5] Rodan Umehara, Harunobu Taguchi, Arata Horie, Yusuke Kamiyama, Shin Sakamoto, Hironori Ishikawa, and Kouta Minamizawa. FEELTECH Wear : Enhancing Mixed Reality Experience with Wrist to Finger Haptic Attribution. In *ACM SIGGRAPH 2024 Emerging Technologies*, SIGGRAPH '24, New York, NY, USA, 2024. Association for Computing Machinery.

[6] DOCOMO Participates in MWC Barcelona 2024. https://www.docomo.ne.jp/english/info/media_center/event/mwc24/.

[7] Yufan Zhu, Ximing Shen, Arata Horie, Yoshihiro Tanaka, and Kouta Minamizawa. EmbodyCraft: Exploring Haptic Embodied Experiences for Reflective Practice in Throwing Clay. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '25, New York, NY, USA, 2025. Association for Computing Machinery.

[8] Tsugumi Sato, Hikari Yukawa, Kouta Minamizawa, and Yoshihiro Tanaka. Co-Operation of a Dual-Arm Robotic Avatar Through Body Integration of Multi-Person. In *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 1030–1036, 2023.

[9] ムーンショット目標 1　身体的共創を生み出すサイバネティック・アバター技術と社会基盤の開発. https://www.jst.go.jp/moonshot/program/goal1/13_minamizawa.html.

[10] Yukiko Horikawa, Takahiro Miyashita, Akira Utsumi, Shogo Nishimura, and Satoshi Koizumi. Cybernetic Avatar Platform for Supporting Social Activities of All People. In *2023 IEEE/SICE International Symposium on System Integration (SII)*, pp. 1–4, 2023.

[11] 金岡晃, 森亮太, 大塚航世, 倉﨑翔大, 大木哲史, 大東俊博, 磯原隆将. VR/AR 環境におけるセキュリティ脅威と攻撃対象領域の体系的分析. 2025 年暗号と情報セキュリティシンポジウム（SCIS2025）, 2025.

[12] Microsoft. The STRIDE Threat Model. https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

[13] Rafiullah Khan, Kieran McLaughlin, David Laverty, and Sakir Sezer. STRIDE-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, 2017.

[14] Mario Hermann, Tobias Pentek, and Boris Otto. Design Principles for Industrie 4.0 Scenarios. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 3928–3937, 2016.

[15] Publications Office of the European Union. Era industrial technologies roadmap on human-centric research and innovation for the manufacturing sector. https://op.europa.eu/publication-detail/-/publication/4a5594d1-4ee3-11ef-acbc-01aa75ed71a1, 2022.

[16] B. Ajay Abishek, T. Kavyashree, R. Jayalakshmi, S. Tharunkumar, and R Raffik. Collaborative Robots

and Cyber Security in Industry 5.0. In *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, pp. 1–6, 2023.

[17] Amal Yousseef, Shalaka Satam, Banafsheh Saber Latibari, Jesus Pacheco, Soheil Salehi, Salim Hariri, and Partik Satam. Autonomous Vehicle Security: A Deep Dive into Threat Modeling, 2024.

[18] Collaborative Robotics. `https://www.co.bot/`.

[19] Fumio Shimpo. Authentication of cybernetic avatars and legal system challenges; with a view to the trial concept of new dimensional domain jurisprudence (ai, robot, and avatar law). *Japanese Society and Culture*, Vol. 6, No. 1, p. 3, 2024.

[20] Aleksandra Pawlicka, Michał Choraś, and Marek Pawlicki. The stray sheep of cyberspace aka the actors who claim they break the law for the greater good. *Personal and Ubiquitous Computing*, Vol. 25, No. 5, pp. 843–852, 2021.

[21] Center for Internet Security. Election Security Spotlight – Cyber Threat Actors. `https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors`.