科学研究費助成事業（基盤研究（Ｓ））研究進捗評価

課題番号	16H06302	研究期間	平成２８(2016)年度 ～令和２(2020)年度
研究課題名	メディアクローン攻撃を防御するコミュニケーション系	研究代表者 （所属・職） （令和３年３月現在）	馬場口　登 （大阪大学・工学研究科・教授）

【令和元(2019)年度　研究進捗評価結果】

評価		評価基準
	A+	当初目標を超える研究の進展があり、期待以上の成果が見込まれる
○	A	当初目標に向けて順調に研究が進展しており、期待どおりの成果が見込まれる
	A－	当初目標に向けて概ね順調に研究が進展しており、一定の成果が見込まれるが、一部に遅れ等が認められるため、今後努力が必要である
	B	当初目標に対して研究が遅れており、今後一層の努力が必要である
	C	当初目標より研究が遅れ、研究成果が見込まれないため、研究経費の減額又は研究の中止が適当である

（意見等）

本研究は、メディア処理技術によって本物ではない音声・画像・映像メディア（メディアクローン（MC））が作り出され悪用される可能性に対して、受け手を防御する技術の構築を目的としている。

進捗状況は順調であり、例えばフェイク情報生成の防止法として、指の写真から指紋、静脈情報が復元されるのを防止する手法や、画像中の外見情報を匿名化する手法が示されている。発話顔と全身動作の動画他のクローン生成を検証するとともに、フェイク動画を認識する手法が与えられている。人がだまされる際の対話のモデルも検討され、さらに MC 生成と認識の実証実験、データベースの公開、報道発表などの研究成果の公表・普及も行われている。

独自性の高い本研究の全ての目標が最終的に達成されるように一層の展開が期待される。

【令和３(2021)年度　検証結果】

検証結果	
A	当初目標に対し、期待どおりの成果があった。 本研究は、本物に限りなく近いが本物ではない音声・画像・映像・テキストなどのメディア（メディアクローン（MC））の攻撃から受け手を防御するメディア技術の構築を目的とする。そのコミュニケーション系の構成要素となるフェイク情報化の防止法（生体・プライバシー情報などの匿名化)、MC 生成法と認識法、MC 攻撃のモデリングの提案と有効性が示され、安心で信頼されるメディア・コミュニケーションの可能性を対戦型循環実証実験により検証されている。特に音声クローンの実証実験に大きな成果があり、新たに認識器クローンなどの研究テーマが生まれている。また、MC のデータベース公開、MC 生成技術を競う国際チャレンジなど、本研究が加速される環境も整備され、当初の計画どおりの成果が達成されている。学術的・社会的に重要なテーマであり、一層の展開が期待される。