ウクライナ「AI 顔認識」の衝撃

～死亡者や侵入者の特定に利用される AI 顔認識の可能性～

ライフデザイン研究部 主席研究員 柏村 祐

1.ウクライナで利用されるAI顔認識

2022 年 2 月 24 日にロシアがウクライナに侵攻を開始して約 9 カ月が経過し、未だその戦況の行方は混とんとした状況が続いている。

ロシアによるウクライナへの軍事侵攻においては、戦闘機、戦車、長距離ミサイルなどさまざまな物理的な兵器が利用されてきた。このような物理的な兵器の活用により戦争が長期化するなか、ウクライナでは、国内で死亡したロシア兵や捕虜となったロシア兵の本人確認を行う手段の1つとして､AI 顔認識が活用されている｡そもそも、ウクライナ政府が AI 顔認識を利用することになったのは、2022 年 3 月 1 日に米国の事業者がウクライナ政府に AI 顔認識の活用を提案したことがきっかけである。その事業者は、ウクライナ政府に送った書簡の中で、AI 顔認識は、写真だけで瞬時に人物を特定できる仕組みであり、インターネットから収集された 100 億を超える写真と照合できると説明している（注 1）。本稿では、ウクライナで活用されている AI 顔認識の実態を概観し、その価値について考察を加える。

2.ウクライナにおける AI 顔認識の活用実態

ウクライナで活用されている AI 顔認識は、侵入者の特定、死亡者、フェイクニュースとの戦い、家族との再会といった様々な用途に利用が進んでおり、その概要は図表 1 の通りである。

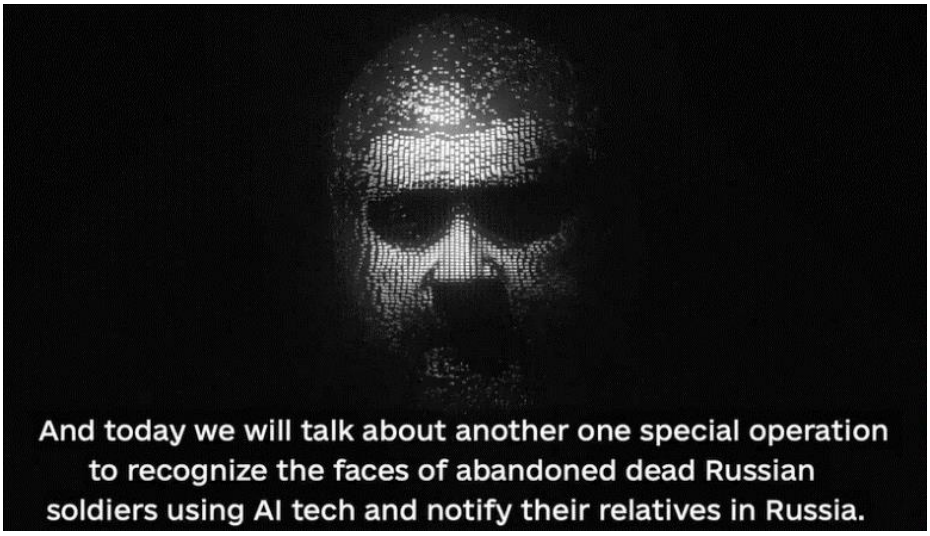
図表 1　AI 顔認識の活用シーンと概要

活用シーン	概要
侵入者の特定	ウクライナを支援するふりをしている可能性のある侵入者は、写真または身分証明書を撮るだけで、リアルタイムで即座に精査できる。
死亡者	顔認識 AI は、取得が困難な指紋を使用せずに死亡者を特定するのに役立つ。 顔認識 AI は、故人の顔面損傷に関係なく効果的に機能する。
フェイクニュースとの戦い	顔認識 AI は、ソーシャルメディアに投稿されるフェイクニュースをリアルタイムで修正するのに役立つ可能性がある。最近の例では、捕らえられたロシア軍兵士が実はウクライナの町ニコラエボ出身のウクライナ人だとする情報がある。顔認識技術を使えば、その 2 つの顔が別人であることを瞬時に識別することができる。
家族の再会	家族と離れ離れになっている難民がいる状況で、顔認識技術により難民キャンプで身分を証明する書類を持っていない人を識別し、家族との再会を手助けすることができる。

資料：Clearview.aiHP「https://app.hubspot.com/documents/6595819/view/443117283?accessId=f27bac」より筆者作成

ウクライナが戦時下で AI 顔認識を活用している事例として、ウクライナのサイバー攻撃部隊である IT ARMY of Ukraine（以下ウクライナ IT 軍）が 2022 年 4 月 5 日に公開した動画をとりあげる。この動画のなかで、人間の顔を模倣した司会者は、くぐもった声で以下のように発言している。「そして今日はもう一つの特別作戦、AI 技術を使って死亡し放置されたロシア兵の顔を認識し、ロシアにいる親族に通知することについてお話します」（図表 2）。

図表 2　人間の形を模倣した「顔」が AI 顔認識を使っていると発言する様子



資料：TelegramSNS より

さらに、実際のAI顔認識の活用方法について、司会者は以下の通り発言する。「AIはソーシャルメディアのアカウントと、友人や親戚のアカウントを探し、インターネット上に同一人物と思われる写真があれば、その写真も探します。次に、親しい人に兵士の死亡を知らせ、遺体の写真を添付します。現在、582 人の遺体を確認し、親族に通知しています」。

また、ウクライナによるAI顔認識の活用は、死亡して放置されたロシア兵の本人確認にとどまらず、戦争犯罪捜査、ロシアの侵入者の特定、検問所でのチェックに活用されている。

戦争犯罪捜査にAI顔認識が活用された事例として、2022年4月25日にウクライナ内務省の第一副大臣イェニン氏が発言した内容が挙げられる。イェニン氏は公式発表の中で、「軍事侵略が始まって以来、ウクライナ国家警察の捜査官は、ロシア連邦とベラルーシ共和国の軍隊の軍人がウクライナの領土で犯した犯罪の事実に基づいて、8,000件以上の刑事訴訟を開始した。152人が拘留され、192人が疑わしいと宣言された」と述べている。この調査にあたっては、ロシア人を特定するために、AI顔認識を利用し、100 億枚以上の写真を含むデータベース内の写真と特定したい人物の画像を比較したとしている（注2）。

次に、ロシアの侵入者の特定に AI 顔認識が有効であったことについてデジタル大臣であるフェドロフ氏は、以下の通り述べている。「顔認識AIの興味深いケーススタディの1つに、ウクライナの病院で発見された男性がいて、彼はシェルショック（砲弾ショック）、または何らかの外傷に苦しんでいるウクライナの兵士であり、すべてを忘れていたと主張していました。そして、彼は自分がウクライナ人だと主張していましたが、医師から写真が送られてきて、数分で彼の身元を特定することができました。私たちは彼のソーシャルネットワークのプロフィールを見つけ、彼がロシア人であることを立証しました。もちろん、彼は責任を問われました。」（注3）

このようにウクライナの戦時下で活用が進むAI顔認識は、使用開始初期の2022年4月時点で、5つの機関と200人の職員が約5,000件程度を検索する規模であった。その後、その有効性がウクライナ国内に浸透したことにより、4か月後の2022年7月には、7つの機関と600人を超える軍関係者がAI顔認識を積極的に使用し、60,000回を超える検索が実施されている（注4）。

3.AI顔認識の可能性

以上のように、ウクライナでは、死亡したロシア兵、戦争犯罪捜査、ロシアの侵入者の特定の身元を特定するためにAI顔認識が活用されている。

一方、この米国発のAI顔認識サービスに利用される顔画像300億枚以上は、インターネット上に公開されているウェブサイト、SNS、その他多くのオープンデータから本人の同意を得ずに収集されているが（注 5）、この収集行動に対して、プライバシー

に抵触するとして各州で対応措置の動きがある。たとえば、カリフォルニア州ではカリフォルニア州消費者プライバシー法に基づいて、州民は自分自身の個人情報を検索できないようにできる（注 6）。また、イリノイ州では生体情報プライバシー法に基づいて AI 顔認識サービスに自分自身が表示されないようにできる（注 7）。

さらに、米国国外においてもこの収集行動に対する対抗措置の動きがある。たとえば、スウェーデンのデータ保護機関である IMY は、数人の従業員が事前の許可なしに顔認識システムを利用したとして警察当局に 25 万ユーロの罰金を科している(注 8)。また、フランスのデータ保護機関である CNIL は、本人の同意を得ずに顔画像を取得していることは EU 一般データ保護規則に違反するとして、フランス領内にいる人のデータの収集と使用を停止するように AI 顔認識事業者に対して申し入れている(注 9)。

現時点で、AI 顔認識サービスの顧客は政府機関のみであり、民間向けのアプリケーションではないと AI 顔認識事業は公言しているが（注 10）、個人の顔という極めて機微性の高い情報を取り扱うため、その活用には慎重な対応が求められるだろう。

AI 顔認識は、インターネットの普及と、ウェブサイトや SNS 上に公開されている顔データを取得する技術の進歩により創造された、従来の常識では考えられなかったテクノロジーである。この AI 顔認識は、戦争のような有事に効果を発揮するツールではあるが、一方で政府機関等が平時でも AI 顔認識を利用する場合、なぜそれを活用するのかを慎重に議論し、国民に丁寧に説明する必要があるテクノロジーといえるであろう。

【注釈】

1) Clearview.aiHP より
https://app.hubspot.com/documents/6595819/view/443117283?accessId=f27bac
2) ウクライナ内務省 HP より
https://mvs.gov.ua/uk/news/z-pocatku-viini-vidkrito-ponad-8-tisyac-kriminalnix-provadzen-shhodo-porusennya-zakoniv-ta-zvicayiv-viini-jevgenii-jenin
3) Clearview.aiHP より
https://www.clearview.ai/ukraine
4) Clearview.aiHP より
https://www.clearview.ai/ukraine
5) Clearview.aiHP より
https://www.clearview.ai/overview
6) Clearview.aiHP より
https://www.clearview.ai/privacy-policy
7) Clearview.aiHP より
https://privacyportal.onetrust.com/webform/1fdd17ee-bd10-4813-a254-de7d5c09360a/a465fd9c-58d4-4793-b5e0-959619d71be7
8) IMYHP より
https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-

cvai.pdf
9) CNILHP より
https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de
10) Clearview.aiHP より
https://www.clearview.ai/principles