

「Man in the middle」

坂口 裕靖

開戦から8ヶ月経ち、いよいよ冬が迫ってきました。そんななか発電施設等に対する執拗な攻撃があり、厳しい冬になりそうです。なんかこいつら、本当に地面以外興味ないんだなと感じます。「人間はさ、根絶やしにしといて後から撒いとけばなんとかなるから、うん、うん。とにかく領土」とか思ってるのだろうか。恐ろしい隣人だ。ダーティボムとか言ってるが...

さて、仕事の都合で全く知らない街に行くことを考えてみてほしい。知り合いは一人もおらず、仕事の関係者は名前を聞いてるけど会ったことも話したこともなく、メールでアポイントを取ってるだけの状況。自分は誰一人その街の人を知らず、その街の誰もが自分のことを知らない。最初に自分のことを認識するのはビジネスホテルだか民宿だかの、つまり泊まる場所に関連

した人ということになる。この人たちは自分の顔と名前を紐づけて認識することができる。まあ仕事場と宿の行き来に加えて、食事したり買い物したりするだろう。その街がさほど大きく無いのであれば、来訪者であることはたちまち判明する。やがて一人二人と顔見知りが増えていくだろう。こちらから見れば顔見知りだが、向こう側は既存の人間関係により結びついている。そうすると「あんた、こないだあそこにおいたら？」とか声を掛けられるようになってくる。これがすなわち「面が割れる」ということだ。個人を姿かたちで識別し、その行動ログをその街の人間ネットワークが共有するようになる。名前も住所も年齢も性別も知らなくとも、その対象を識別さえできれば、その行動を追いかけて突合することが可能になる。片方が持っている情報と

もう片方が持っている情報を持ち寄ると、その対象がどこからどこへ、どういう意図を以て行動したかがわかるようになる。やがて名前や住所や年齢・性別などの情報が入手されるとともに、その対象に対して属性がべたべたと貼り付けられていく。「あの仕事で来た人」から「なんたらさん」と呼び方は変わるが、同じ対象を指していることは変わらない。そして、実はその貼り付けられた属性はあまり意味を持たない。「なんたら」が偽名であろうが通称であろうが本名であろうが、その真贋は割とどうでも良いことだ。なぜなら対象は対象として認識・追跡可能であれば、後日いくらでも訂正可能なのだから。

やがて仕事が終わってその街を後にする日がやってくるだろう。あなたのことが街の人々の会話に登ることが減っていき、や

One Point BUZZ WORD

AI 樋口円香

画像生成AIがオープンソースされ、爆発的広がりを見せる中、想像もしなかったような領域へ展開しつつある。まずは樋口円香がラーメンを食べる画像が衝撃を与えた。ラーメンや箸という概念をうまく咀嚼しきれてないAIは、手づかみでラーメンをはむはむ食べるという、人智の及ばぬ画像を生成したのだ。あの煮えたるラーメンを手づかみで食べるという場面を想像したことがある人類は一人でもいただろうか。そんな画像を見たことが、描いたことがあるだろうか。これが呼び水となり、可能性が追求される。「ゲーミングちんぼ華道部」とか「ケーキ女の子」とか「爆乳機関車」とか「プリンセスペニス盆栽」とか、AIが人類性癖の極北をざくざくと切り開きつつある。今となっては、なんで今

までこれらの領域が探り当てられなかったのかが不思議なぐらいだ。が、そこいらへんは絵を描く才能と言葉を操る才能が微妙に異なるあたりにあるのかもしれない。つまり「庭付きプール付き腕時計」とかの意味空間でしか存在し得ないワーディングで遊んでた向きには、説得力ある絵としてこれを実現できる人がいなかった。一方説得力ある絵は具現の積み重ねであり、具現の積み重ねで抽象を描く方向が深すぎて「爆乳機関車」ぐらいの抽象度でやめとくことができなかったのだろう。少なくとも現在のAIは、言葉を理解するが、意味は気にせず具象を積み上げることができると、ワーディングをするってそれなりに説得力のある絵にしてしまう。結果人類性癖の新たな地平線が切り開かれたというわけだ。...いや...まあもしかしたら人知れずコツコツと「爆乳機関車」してたヒトがいるかもしれませんが...世界は広いので...まあでも、AIが増幅したことは間違いないだろう。これからも言語空間と画像空間の見たこと無いような暗黒魔合体が日本から続々と生まれていくのではないだろうか。それだけの豊かさがキャラ弁の国・日本にはあると信じたい。

がてあなたがいた事を知ってるものもいなくなるだろう。次の仕事で訪れる街でも似たようなことが繰り返されるだろう。

さて、そんななか、ある特定の顔認識システムが広く薄く全国に導入されていたとしてみよう。このシステムは顔認識により対象を特定し、認識した日時と場所をログとして記録する。そしてその記録はシステムを採用している全ユーザーで共有されるとしてみよう。これは薄く広がった、行ったことがなかった街と全く同じ状況だ。どここのファーストフードに何月何日何時頃現れ、それから数時間後にデパートを訪れてる、といった情報が顔に紐づいて蓄積されていく。どこかの施設では、その顔と会員情報が紐づくかもしれない。実際にどここの誰かがそれによりわかるかもしれないが、実はそれは些末な問題だ。どういう行動を取っていたかの記録こそがその対象を表しており、属性はさほど重要ではない。追跡できることが重要であり、過去の行動がわかることが重要なのだ。我々の社会が特定の行動を起こした人間を忌避するのも、これが理由であろう。名前は未捕捉の対象を捕捉するために役立つが、問題とするのは名前ではなく、過去の行動履歴である。

ところが、過去の行動履歴は未来の行動を規定するものではない。未来の行動を予測する上で過去の行動履歴はそれなりのウェイトを占めるとは思うが、過去の行動からのみ予測できるというものではない。通販サイトで枕カバーを買うと、枕カバーに関する広告がドカドカ出るようになるかもしれないが、多分その人は当分の間枕カバーを買うことはないだろう。まあ邪魔な広告ぐらいなら笑って済ませるのだが、過去の行動履歴から人物を想定し、邪険な扱いを受けるようになるのだとしたら大変な問

題である。そして、そういうことはここそこで頻発しており、楽観を許さない。問題となるのは追跡をすることではなくて、追跡した結果をもとに何らかの未来を予測し、その予測した未来で判断が下され、やってもないしやるつもりもないことを理由として不利益を被りうることにある。そして、システムアップされた現代では、その一度の判断が決定的な意味を持つことが少なくない。まあ行動履歴から将来の行動を予測して判断することをしないのであれば問題ないのだが、だったら行動履歴を保存する必要はないはずであり、またそういうデータが手元があればなんか使いたくなるのは人間の本性といっても良いだろう。だからこと、手元にあるデータの扱いには慎重にならなければならない。「図書館の自由に関する宣言」が利用者の秘密保持を謳う理由がここにある。図書館の履歴をつなぎ合わせると、誰がどの本をどの順番で読んだのかを追跡することができる。複数の図書館で利用履歴を突合すれば、さらに詳しい情報となるだろう。銃器の構造や原理、材質や加工方法などの本を読み進めていた場合、それが何を意味するのだろうか。銃器を作って発砲することを考えていたのかもしれないし、銃器を作るための新しい工作機械を設計するに当たり、情報を集めていたのかもしれない。あるいは小説家がガンズミスのキャラクターを作るための基礎資料として閲覧していただけかもしれない。過去の行動履歴から意図を汲み取ることは基本的に不可能だ。銃撃という行動を遡ってこれら資料の閲覧が出てきたからといって、これら資料の閲覧という行動履歴が常に必ず銃撃という将来の行動に結びつくわけではない。それでも「行動履歴から意図を汲み取れる」と信じる向きは一定数おり、そ

れなりの発言力をもつ場合が多い。というわけで、顔認識が広く薄く浸透することに対して違和感が表明されているわけだ。先の見知らぬ街のように、導入した店舗とかのレベルで強かに囲い込まれ、かつ他と履歴を共有できないのであれば問題はないかもしれない。しかしフランチャイズ本部にとって万引きした人間を認識したい、横展開して予防したいという欲求を抑えることは難しいだろう。システムだってタダじゃないんだし。というわけで、そういう地獄を招きかねないから顔認識はやめてくれ、ということになるわけだ。これは漏洩の問題ではなく、自分の知らないところで行動履歴が勝手に作られ、共有され、ありもしない未来を想像され、取り返しのつかないことが起こると嫌だ、という問題なのである。

さて、でマイナンバーカードだ。顔認識は顔の画像情報などから個人を識別するものであるから、当然完全では無いだろう。一方マイナンバーはすべての住民に割り当てられた唯一無二のIDであり、しかも一生変わらない。マイナンバーを追跡することで、対応する人間を確実に追跡可能だ。だからこそ、マイナンバーを利用できる局面が法律できっちり限定されてるわけだ。なんだけども、マイナンバーカードはマイナンバーを機械的に読み取り可能であり、その機械がどう内部処理（例えば、マイナンバーをこっそり送信するとか）がわからないという問題がある。だからいきなり保険証って言われると大変もによる... その利用局面を決める法律すら、いつどう変わるかわからんし。実際変わったし。

Hiroyasu Sakaguchi
株式会社 IMAGICA Lab.