Trend Micro Research

一度漏えいした情報は一生悪用される ソーシャルメディアにおける生体情報漏洩が将来に及ぼす影響

Craig Gibson, Vladimir Kropotov, Philippe Z Lin, Robert McArdle, Fyodor Yarochkin

はじめに 3

何が露呈しているのか? 6

人々に及ぼす影響：現在と将来の攻撃シナリオ 33

読者の皆様に伝えたいこと 47

まとめ 51

付録 53

はじめに

私たちはソーシャルメディアを利用して、友人や親戚と連絡を取り合うことや、世界中の人々に自分のことを知ってもらうこともできます。自分たちの経験を、写真や動画、音声といった形で共有して楽しんでいます。ただし残念なことに、個人的なメディアコンテンツを共有することで、機密性の高い生体情報を露呈してしまっていることも少なくありません。たとえば、Instagram では#EyeMakeup というハッシュタグを付けた投稿が 1,000 万件近くあり、TikTok では#EyeChallenge というハッシュタグを付けた動画の再生回数が 20 億回を超えています。一方で、これらのハッシュタグはどちらも、虹彩パターンの情報を露呈しているユーザであることを示しています。

10 年前に比べて、今日の生体認証テクノロジは私たちの生活の中ではるかに重要な役割を果たすようになっています。たとえば次のような日常的なシナリオで、生体認証テクノロジが使用されています。

- 自動化されたシステムを使い税関等の出入国管理システムを通過する
- 銀行口座のロックを解除して ATM から現金を引き出す
- 次世代的な技術を導入しているスーパーで食料品を購入する
- 生体認証センサ付き公共交通機関で料金を支払う

これらのシナリオを念頭に置くことで、私たちの生活の中で生体認証テクノロジが果たす役割を明確に理解できます。さらに重要なのは、これらの出来事は特定の状況で発生し、ユーザに対してはっきりとした影響をもたらすという点です。たとえば、自動化された出入国管理システムを通過するユーザは、システムによって認識された場合はそのまま進むことを許可されますが、認識されなかった場合は警告が表示されて足止めされる可能性があります。

一方、指紋認証や顔認証でスマートデバイスのロックを解除するときのように、その行動があまりにも日常的で、1 日に何度も生体情報を使用していることにほとんど気付かないシナリオもあります。指で正しくセンサに触れる、スマートデバイスのカメラをちゃんと顔のほうに向ける、といった一定の動作を行う必要があるとしても、これらの動作は自然で、ほとんど無意識に行われます。

しかし、私たちがソーシャルメディアで上述のような種類のコンテンツを共有して公開すると、攻撃者に私たちの生体情報を入手する機会を与えることになります。音声メッセージを投稿することは、声紋情報を露呈するということです。写真や動画を投稿することは、顔、網膜、虹彩、耳介などのパターン情報を露呈するということであり、場合によっては掌形や指紋を露呈することになります。

投稿したデータには誰でもアクセスできる可能性があるので、そうした情報の拡散を完全に制御することはできません。したがって、そのデータにすでにアクセスしているのは誰なのか、いつまで保持されるのか、何のために保持されるのかを知ることはできません。

このデータには多くの課題があり、現在の利用状況ではそれらの課題の重要性は一段と高まっています。現在、私たちは、高解像度化したスマートフォンのカメラ、4K 動画や高解像度写真に対応したメディアプラットフォーム、およびクラウド、データマイニング、AI、機械学習（ML）の各機能など、新しい技術の組み合わせによって、セキュリティリスクが大きく変化する転換点にあります。

このイノベーションのるつぼにより、すでに特定の用途で生体データが使われ始めています。たとえば、監視カメラで人物を追跡する場合に使用する顔認識アルゴリズムは、本人がこれまでにソーシャルメディアにアップロードしたデータでトレーニングします[1]。サイバー犯罪者は、それと同じデータをソーシャルメディアから取得して、ID 窃盗攻撃やディープフェイク（特に公人のディープフェイク）の作成に利用できます。

同じソーシャルメディアデータは、ID 窃盗攻撃にも、政府による監視にも、ディープフェイク（特に公人のディープフェイク）の作成にも利用できます。今のところ、金融犯罪でこれらのデータが利用されることはあまりありませんが、利用できる可能性は上がる一方であり、それに伴って時間の経過とともに悪用の危険性も拡大するでしょう。

一見すると、生体情報はオールインワンソリューションのように見えます。生体情報は、本人確認と認証に使用できる固有のものであり、常に本人と共にあります。数十年にわたって、生体情報は、犯罪捜査や科学捜査の促進、政府施設への出入など、さまざまな特定の用途で使用されてきました。今日では生体情報の役割が拡大し、数億人の人々が日常的に生体情報を使用しています。残念なことに、このことは、それだけの数の人々が、生体データ処理で使用されるテクノロジやプロセスの脆弱性や弱点の犠牲になる可能性があることも意味しています。

トレンドマイクロは、リスクを評価するために、現在または近い将来に生体情報を利用しかねない既知のユースケースを調査することにしました。さらに、生体認証システムによる本人確認と認証に使用されている基盤テクノロジについても調査しました。残念なことに、マルチメディアコンテンツを公開する際、このコンテンツがどれほど侵害されやすいか、多くの人が認識していません。当然、そのようなコンテンツの露呈がもたらす現在および将来のリスクも知りません。

本書の目的は、ソーシャルメディアにコンテンツを公開することについてユーザが知っておくべき重要な点、すなわち公開したコンテンツからすでに露呈している、または今後露呈する可能性がある機密情報は何か、そのようなコンテンツの公開が個人の生活だけでなく、生体データを使って処理を行う組織の日常業務にもどのような影響を及ぼす可能性があるかを明らかにすることです。さらに、現在露呈している生体特徴や行動データを使用した今すぐ

[1] https://www.nist.gov/system/files/documents/2020/09/03/10_ntechlab_nist_2016.pdf

にも起こりうる攻撃シナリオについて説明します。最後に、生体データの露呈と使用に関連するリスクを最小限に抑える推奨事項を紹介します。

何が露呈しているのか?

本稿では、露呈しているコンテンツの種類と、そのようなコンテンツがどういったソーシャルメディアプラットフォームで露呈しているか、に焦点を当てます。人々が露呈する特徴は、静的または動的のどちらかです。静的な特徴は、1 つのフォトフレームから取り出すことができ、不正な意図で使用するのに十分な生体情報を露呈している可能性があります。そのような特徴の例として、顔の輪郭、虹彩、網膜、掌形、および指紋があります。

動的な特徴は、動画や音声録音として漏えいすることが多いため、収集に必要な時間が長くなります。動的な特徴の例として、声紋または人々の感情表現の方法があります。これらの情報の多くは、キーボードを使って文字を入力する、ブラウザウィンドウを操作する、手書きで文字を書く、紙に署名するなどといった、人々の行動の癖やパターンを何者かが観察することで露呈します。これらの特徴はすべて、認証と本人確認のどちらにも使用できます。

上述したすでによく知られている特徴の他にも、人々の本人確認または分類に使用できる非生体的な固有の特徴があります。これらの特徴には、母斑やタトゥーのような、分離不能（またはほぼ分離不能）の特徴が含まれます。同様に、衣服やアクセサリのような分離可能な特徴は、社会的身分、民族性、年齢のプロファイリングに使用できます。サイバー犯罪者は、ソーシャルメディアに投稿された有名ブランドの衣服や、サングラス、帽子、バッグなどのアクセサリなどの情報を活用して、そうしたコンテンツをアップロードする人々に攻撃を仕掛けることができます[2]。

また、すべてのコンテンツが意図的に露呈するわけではないので、このセクションでは、コンテンツが露呈しやすい状況についても説明します。たとえば、指紋はミニチュア料理の作り方を説明する動画で露呈することが多く、虹彩パターンはメイクアップ関連のコンテンツで露呈するのが一般的です。これらの種類のコンテンツには、まだ対処されていない多くのリスクが伴います。そのため、メディアコンテンツの所有者、制作者、およびホストの間に、どのような状況が露呈するリスクをもたらすのかについて認識を広めることが最も重要です。

生体情報の非意図的な露呈に関して 10 年前と現在で大きく異なるのは、メディアコンテンツの品質と解像度です。品質と解像度が大幅に向上し、それによって、攻撃者がより高い品質で特徴を抽出し、生体認証登録などの生体認証システムに使用できるようになりました。

コンテンツの種類

現在のソーシャルメディアでよく見られるコンテンツは、写真、動画、および音声録音の 3 種類です。しかし、ここで重要なのは、メタデータ、説明、コメント、およびハッシュタグによってそれらのメディアコンテンツが検索可能になり、それによってそれらを露呈したシチュエーションについてより深い洞察が得られるようになることです。メディアコンテンツ

[2] https://www.nbcnewyork.com/news/local/investigations-i-team-social-media-use-survey-new-york-new-jersey/1329983

自体またはその説明には、行動、気分、および感情に関する情報が含まれることが多く、それらはさまざまな攻撃シナリオにも使用できます。

音声録音

自分の音声メッセージを投稿すると、声紋と共に自分の気分、感情、および背景の雑音が露呈します。録音メタデータからは、録音した日時、場所、および環境に関する洞察も得られます。さらに重要なのは、こうしたさまざまな環境で録音された音声情報のコレクションは、攻撃者がチャレンジレスポンス方式のセキュリティシステムを回避するのに利用できるということです。たとえば、システムが認証のために、ユーザに所定のリストのフレーズまたはランダムなフレーズを発音するように要求する場合、流出した録音情報でトレーニングを行い合成した人工音声を使用して、この要件を回避できます。多くの場合、声が露呈するのは、メッセージングプラットフォームを使用して音声メッセージを送信するとき、または音声トラックを含む動画を共有するときです。

写真と動画

写真や動画のコンテンツでは、顔、網膜、虹彩、耳介に関する情報、場合によっては掌形や指紋が露呈します。

写真は静的です。これは、露呈する情報が行動に関する情報に制限されることを意味します。ただし、多くの場合、写真には、メタデータ、感情に関する洞察、日時、場所、および環境に関する詳細が含まれます。動画は大量の連続写真として扱うことができ、通常は音声トラックを含みます。したがって、写真とほとんど同じ情報が露呈します。ただし、その量は膨大です。動画には行動と環境に関するより詳細なデータに加えて、音声メッセージも含まれています。

3D モデル

音声、写真、または動画の規模のコンテンツでは、身体の 3D モデルは露呈しません。しかし、それらの 3D モデルを抽出するために必要なすべてのテクノロジはすでに確立されており、顔の 3D スキャンを見つけることが可能になっています[3]。

ソーシャルメディアコンテンツがメタバースへ移行すると、3D モデルが大量に出現する可能性があります。これらのモデルは、複製して、生体認証センサをだますために利用できる可能性があります[4]。また、人々は現実世界の自分をよりリアルに表現したものをメタバースのアバターに使おうとするでしょう。

[3] https://sketchfab.com/search?q=tag%3Afacescan&sort_by=-likeCount&type=models

[4] https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/?sh=450b8efa1330

近い将来、監視体制の拡大、仮想現実・拡張現実・メタバース関連テクノロジの広がり、自律配送、顔認識を使用する軍用ドローン[5]、生体情報を取得して利用できる自動運転車など、それらに類するテクノロジによって、人々の身体と行動の生体情報の露呈は増えることが予想されています。

今日、生体コンテンツを露呈しているのはどのソーシャルメディアプラットフォームか?

このセクションでは、さまざまなメディアプラットフォームで露呈するコンテンツの種類を調べます。今日、生体特徴を含む機密性の高いコンテンツが、ソーシャルメディアプラットフォームやメッセージングプラットフォームに定期的に投稿され、公開されています。また、企業や政府のポータルサイトでは、高解像度の肖像写真や雇用主のインタビューなどが公開されていることが多く、誰もが機密データを見つけることができます。

メッセージングプラットフォーム

Viber、Telegram、WhatsApp などのメッセージングプラットフォームは、当初は個人同士の通信に使用されていましたが、現在はグループでの交流に対応するプラットフォームに変化しています。これらのチャネルやグループの多くは、より多くの人々を引き付けるために、意図的にそのコンテンツを公開しています。参加者数は、人気のあるグループでは数万人に達することも珍しくなく、最も有名なチャネルでは数百万人に達することもあります。テキストの投稿と並行して、これらのチャネルやグループのコンテンツは、音声メッセージ、写真、および動画として共有されており、そのようなコンテンツから重要な生体特徴が抽出されやすくなっています。

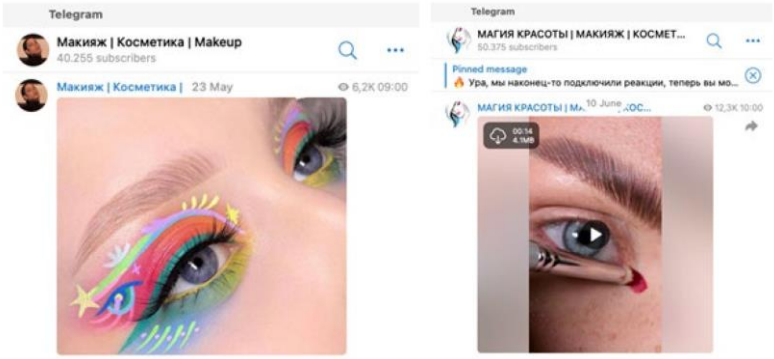


図 1：Telegram[6, 7]で生体特徴を露呈している写真や動画
画像クレジット：Makeup | cosmetics and Magic of beauty | make up | cosmetics/Telegram

[5] ttps://foreignpolicy.com/2021/07/05/killer-flying-robots-drones-autonomous-ai-artificial-intelligence-facial-recognition-targets-turkey-libya
[6] https://t.me/ideyaka/2226%20
[7] https://t.me/makiyazh3/8677

ソーシャルネットワーク

Facebook、V Kontakte、OK（ヨーロッパで人気）などのソーシャルメディアネットワークは、さまざまなマルチメディアコンテンツをサポートしています。当然、そのようなコンテンツには顔の写真が含まれています。それらのコンテンツからは、虹彩パターン、耳介、掌形、指紋、さらには声紋も抽出できます。それに加えて、特定の日時に訪れた場所、住居環境などの詳細な環境情報は、個人の位置情報を取得し、深くプロファイリングするのに役立つ可能性があります。こうした情報が、多くの場合、露呈したコンテンツからも入手および抽出できることは注目に値します。

不正な意図を持つ人物またはグループは、簡単な検索を実行して、生体特徴を露呈するマルチメディアコンテンツを見つけることもできます。図 2 は、Facebook で「eye close-up」を検索した結果を示しており、目と虹彩パターンがはっきり露呈しています。

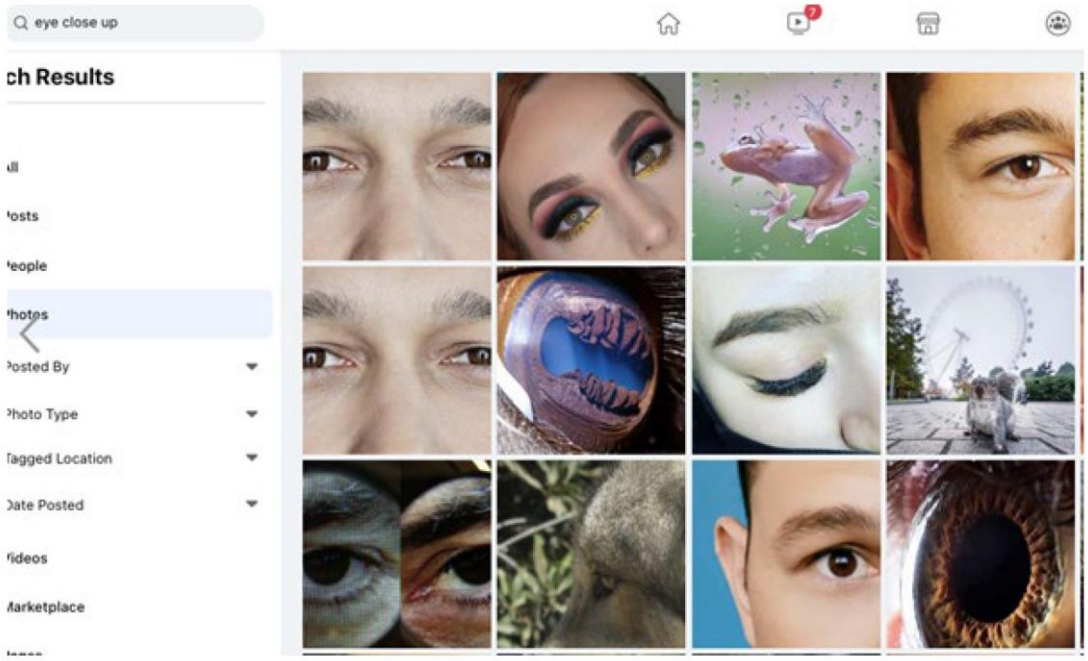


図 2：Facebook で「eye close-up」を検索した結果

Instagram

Instagram は、視覚メディアが中心のプラットフォームであり、個人の活動を示すコンテンツが大半を占めています。プロフィールの人気は、フォロワー、コンテンツビュー、コメントなどのエンゲージメントの数によって左右されます。投稿には、宣伝や同様のコンテンツの検索に使用できるハッシュタグを付けることができます。人気獲得競争のために、プロフィール所有者は、プロ用の撮影・録画・照明機材を使用して制作された、高品質なメディアコンテンツを公開するようになります。しかし、このようなコンテンツの高品質化は、それが露呈した場合に生体特徴の抽出に使用しやすくなることも意味します。

図 3 では、ハッシュタグ#Earrings を付けたコンテンツのサンプルを宣伝する際に、間接的に（非意図的に）耳介が露呈しています。以降のセクションでは、これまでに説明した種類のソーシャルメディアコンテンツにおける生体特徴の意図的な露呈と非意図的な露呈の両方について説明します。

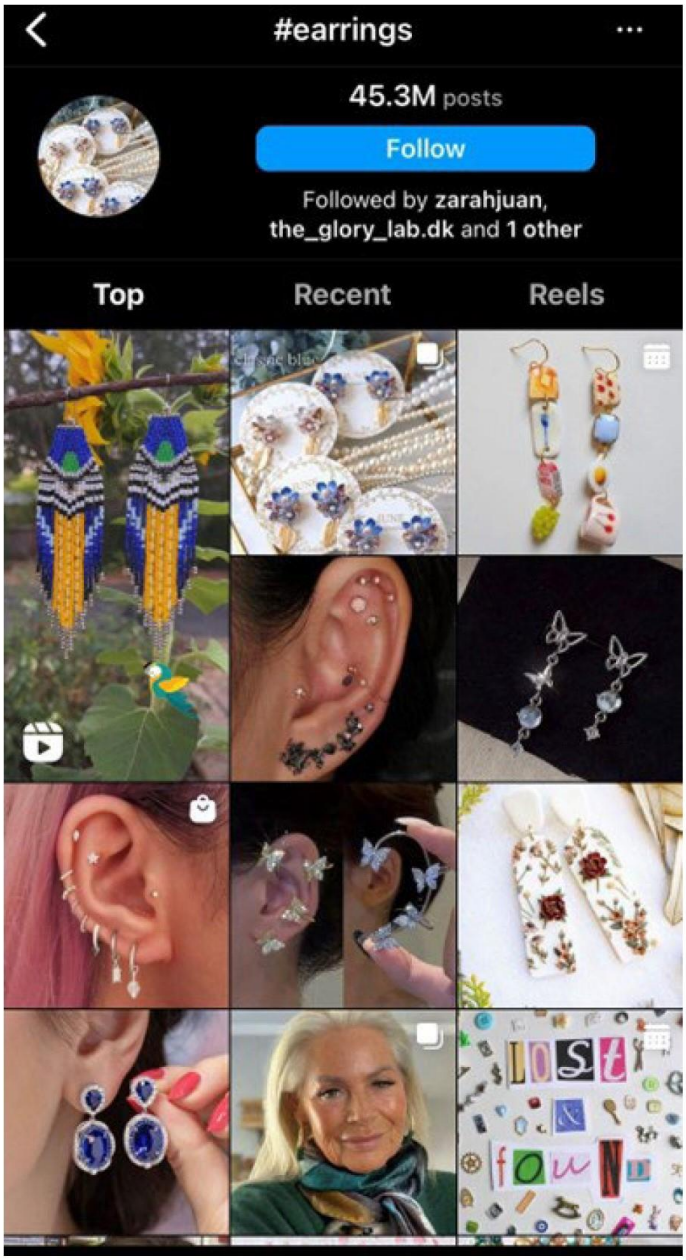


図 3：Instagram でハッシュタグ#Earrings で得られる耳介の露呈の例

TikTok

TikTok は、フォロワー数、動画視聴回数、および「いいね」などのエンゲージメントによって人気が左右される、動画コンテンツが中心のソーシャルメディアプラットフォームです。Instagram と同様に、投稿、動画で使用される音声トラック、およびトピックのトレンドは、ハッシュタグによって左右されることがよくあります。ユーザはやはりプロ用機材やスマー

トフォンの高解像度カメラを使用してさまざまなコンテンツを録画でき、その大部分は未登録ユーザでもアクセスできるように公開されます。Instagram と同様に、ユーザはハッシュタグを使用して興味のあるコンテンツを見つけることができます。

図 4 は、掌形や指紋が露呈しているスクリーンショットです。

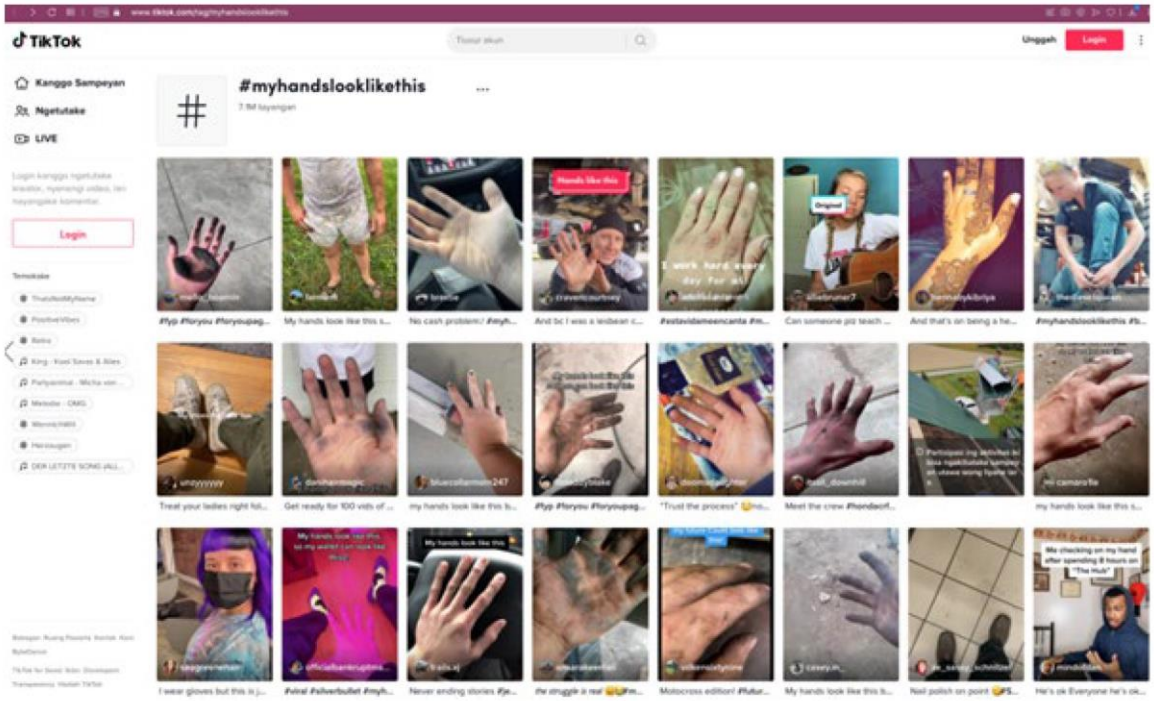


図 4：TikTok でハッシュタグ#MyHandsLookLikeThis で得られる手のひらの例（#JazzHands トレンドとも呼ばれる）。掌形や指紋が露呈する可能性がある

YouTube

YouTube は、1 日あたりの動画再生回数が 50 億を超える動画ホスティングプラットフォームです[8]。このプラットフォームではコンテンツの種類に特に注目することはありませんが、生体データを意図的／非意図的に露呈する動画がここでも公開されています。

YouTube にアップロードされる動画は、ここ数年で高品質化しています。現在、ほとんどの動画は少なくともフル HD の解像度でアップロードされており、プロのコンテンツクリエイターは、4K あるいは 8K のウルトラ HD 解像度の動画をアップロードしています。注目すべきこととして、無論ウルトラ HD 解像度の動画のほうが生体特徴を収集されてしまう可能性が高いのですが、フル HD 解像度でも接写レンズで目を撮影しているシーンなど、十分に生体特徴が取得されてしまう解像度を持つ可能性があります。

図 5 の一連の画像は、目を露呈している例です。これらは「blinking eye」（まばたきする目）を検索して得られた画像です。

[8] https://fortunelords.com/youtube-statistics

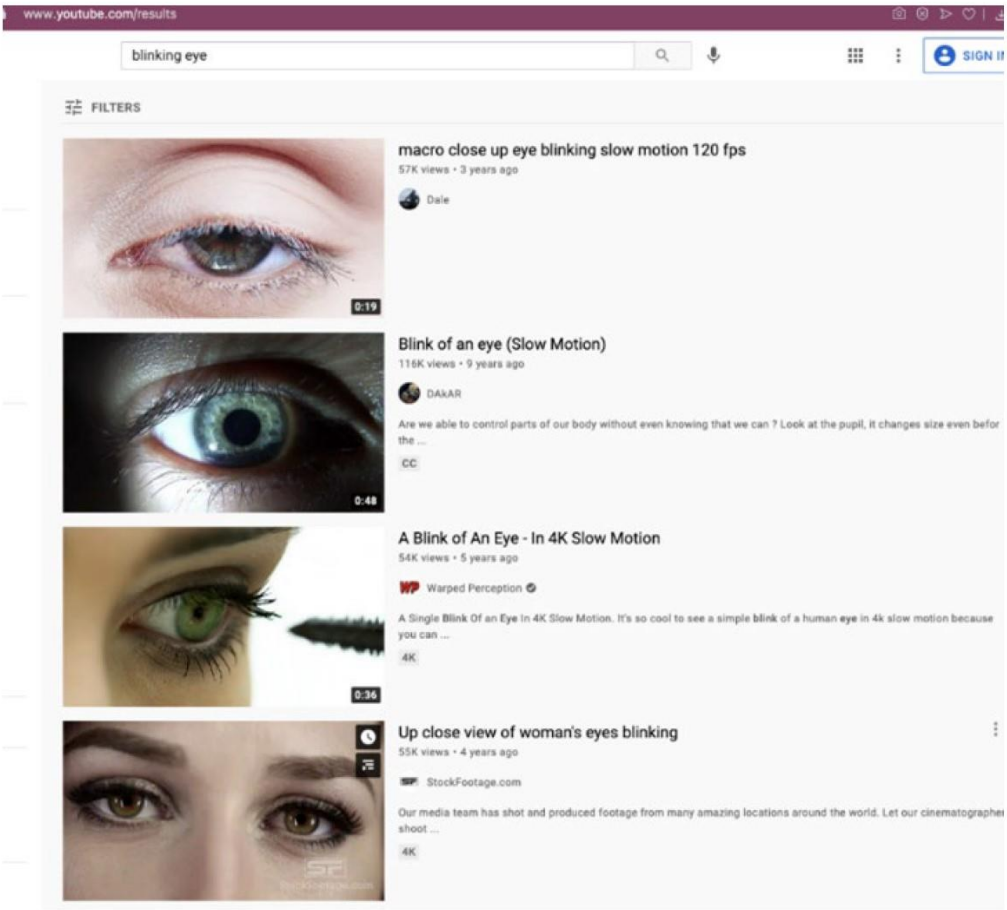


図 5：YouTube における目の露呈

Twitter

Twitter は、主にショートメッセージを投稿するのが目的ですが、写真や動画を添付することもできます。ユーザは、プラットフォームの検索語としてハッシュタグやフレーズも使用できます。コンテンツは、通常は認証不要でアクセスでき、検索エンジンにより索引が付与されています。メディアコンテンツの品質はさまざまですが、このプラットフォームでも露呈している生体パターンを見つけることができます。

Twitter における露呈の規模は、明らかに他のソーシャルメディアプラットフォームほど大きくありませんが、だからといって露呈が全く起きないというわけではありません。図 6 は、露呈している指紋の例です。

図 6：Twitter で露呈している指紋[9]
画像クレジット：SerScience/Twitter

企業および政府の公式ポータルサイト

企業および政府の公式ポータルサイトは、強い影響力を持つインフルエンサーや意思決定者がそのメディアコンテンツに登場するので、露呈しやすいカテゴリに属します。たとえば、欧州委員会の公式サイトでは、政府高官の肖像写真が 10 MP 以上の解像度で公開されています[10]。

キーワード、カテゴリ、日付範囲などのパラメータを使用して検索を実行すれば、政府高官の 5 万枚以上の写真と 12 万本以上の動画が見つかるでしょう。動画はさまざまな解像度で提供され、その音声トラックは別ファイルとして提供されています。

[9] https://twitter.com/science_ser/status/1537322831813431296
[10] https://audiovisual.ec.europa.eu/en/search?mediatype=PHOTO&categories=Portrait

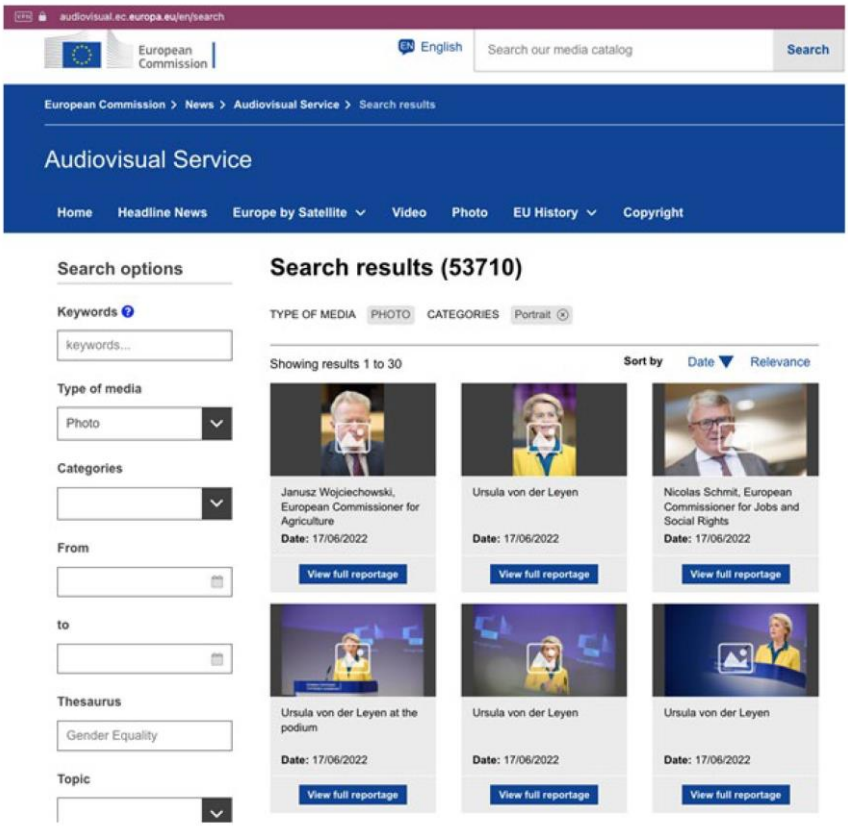


図 7：欧州委員会ポータルで肖像写真を検索した結果[11]

提供されているメディアコンテンツには、日時、場所、タグ、個人情報（名前）などの詳細なメタデータが設定されており、露呈しているそれぞれのコンテンツの ID もわかります。

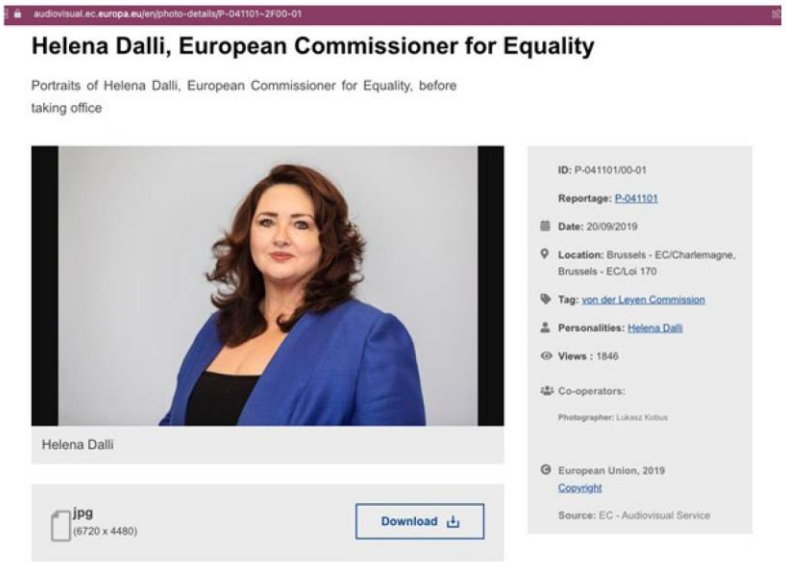


図 8：Europa.eu Web サイトの解像度 28 MP（6720 × 4480）の肖像写真および詳細なメタデータと説明[12]
画像クレジット：欧州委員会

[11] https://audiovisual.ec.europa.eu/en/search?mediatype=PHOTO&categories=Portrait

[12] https://audiovisual.ec.europa.eu/en/photo-details/P-041101~2F00-01

政府および企業の公式ポータルに載せるメディアコンテンツは、プロが最高級機材を使用して作成します。したがって、メディアは非常に高品質であり、画像のほんの一部からでも、そこに露呈している生体特徴を鮮明に収集できるだけの十分な解像度があります。

図 9：欧州委員会の公式ポータルの高解像度写真の隅に露呈している手の形[13]
画像クレジット：欧州委員会

ニュースサイトおよび報道メディア

ニュースサイトを見て回ると、ここでも生体情報を露呈している高解像度メディアを見つけることができます。特に政治家、CEO、および有名人の高品質写真は、予想どおりに見つけることができます。多くの場合、さまざまな記事の写真や内容から、その写真の人物、日時、場所、撮影環境に関する詳細な情報を得られます。次の図の左側には、ニュースポータルでよく見られる写真の表示とそのパラメータを示しています。右側には、ニュース画像に通常付加される広範囲に及ぶメタデータの例です。

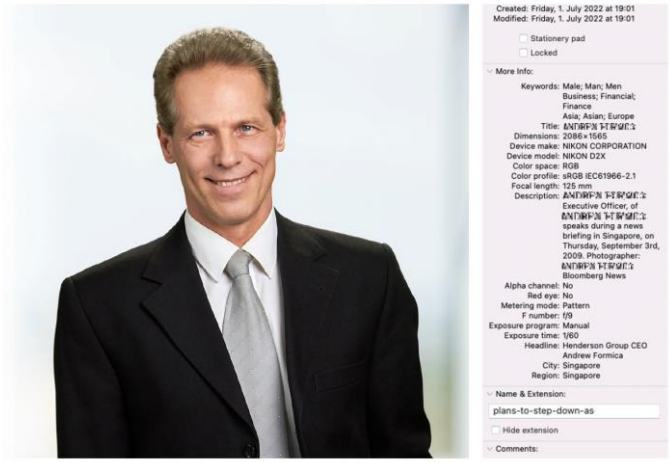


図 10：Bloomberg ニュースポータルなどのニュースサイトで見られる写真の表示[14]。顔、耳、および虹彩情報が露呈し、画像にメタデータが添付されていることがわかる

[13] https://audiovisual.ec.europa.eu/en/photo-details/P-057062~2F00-49

[14] https://www.bloomberg.com/news/articles/2022-06-28/formica-plans-to-step-down-as-jupiter-ceo-beesley-to-take-over

たとえば、インタビュー対象者が脇に座る、影に隠れる、マスクを着用するなどの方法で匿名であろうとする特別なケースは存在します。しかし、そのようなケースでも、生体特徴や個人が特定できるような特徴が露呈し、インタビュー対象者が特定される可能性があります。

匿名インタビューの場合、特定のインタビューに答えるために必要な情報を持っているのはほんの一握りの人のみであるという事実を考慮する必要があります。その場合、インタビュー対象者の ID が、インタビュー中に露呈する見た目の年齢、性別、および身長に従って絞り込まれる可能性があります。同時に、画面上でカモフラージュを施したり、目だし帽やマスクを着用したりしても、機密性の高い特徴が非意図的に露呈する可能性があります。

オンラインニュース記事の場合、オンライン記事に含まれる低解像度の写真はそれほど有害ではありません。ただし、同じポータルサイト内に高解像度の写真が置いてあることが多く、URL の一部（倍率など）を削除または変更することによってそれらを抽出できます。

図 11 は、生体認証システムの虹彩認識登録に十分な鮮明さを持たない画像の例です。ただし、The Sunday Times に掲載された同様の画像を見てみると、サイトを少し変更するだけで高解像度の写真（この場合は 20 MP）が表示されます。この写真は、画像内の人物を特定する、またはその人物になりすますのに十分な詳細情報を露呈する可能性があります。記事[15]に元画像が含まれていますが、これを新しいタブで開くと、約 1.2 MP の解像度の画像[16]を表示できます。さらに、倍率を削除して新しいタブで開くと、約 20 MP の解像度の画像[17]も表示できます。

状況によっては、虹彩パターンが過去に漏えいした、または画像から取得できた場合、税関などの出入国管理の生体認証システムで利用されたり、特定の建物に出入するために利用されたりする可能性があります。

図 11：固有の顔の詳細および目を露呈する可能性がある The Sunday Times の画像

[15] https://www.thetimes.co.uk/article/british-army-creates-ranger-regiment-k0kfckkw3

[16] https://www.thetimes.co.uk/article/british-army-creates-ranger-regiment-k0kfckkw3

[17] https://www.thetimes.co.uk/article/british-army-creates-ranger-regiment-k0kfckkw3

別の例を、図[12]の一連の写真に示します。これは、集会や抗議行動のニュース報道でよく見られる画像の表示です。仮面を付けている人物は、虹彩情報と顔の輪郭をうまく隠すことができていますが、一方で耳介、掌形の一部、およびタトゥーを露呈する可能性があります。露呈したこれらの特徴を個別または一括で取得することで、人物を特定する可能性が大幅に高まります。これは複数の人物がすでに識別されている特定の既知のグループのうちの１人を識別することが目的である場合、顕著に当てはまります。主に後頭部が写る位置にカメラが設置されていたとしても、いくつかのカメラアングルで耳介やタトゥーが露呈する可能性があることに注意する必要があります。

図 12：顔が見えなくても耳介やタトゥーが露呈する可能性がある。
ニュース報道でよく使用される写真[18]の画像

画像からそのような人物を特定することは、簡単な作業ではありません。しかし、ある地域に存在した人々に関する通信ネットワークデータや、同じ固有の特徴を露呈しているソーシャルメディアの投稿など、可能性のあるさまざまなソースを組み合わせると、何も露呈していない状況に比べて、特定できる可能性は大幅に高くなります。

検索エンジン

検索エンジンは、通常はコンテンツの索引を作成し、さまざまなソースで公開されている複数のメディアを相互に関連付けることができます。たとえば、写真に写っている人物にタグを付けることで、生体特徴も含んだより解像度の高い類似した写真を見つけることができます。

Google、Bing、Yahoo、Yandex、および Baidu は、広く使用されている検索エンジンです。しかし、tgstat.ru のように、特定のソーシャルメディアまたはメッセンジャーネットワークのみを対象とする検索エンジンもあります。また、social-searcher.com のように、ユーザがソーシャルメディアプラットフォームを検索できるようにするエンジンもあります。しかし、検索エンジンは通常コンテンツの露呈の責任を負いません。したがって、特定の人物の

[18] https://www.spiegel.de/netzwelt/netzpolitik/anonymous-und-guy-fawkes-grinsemaske-ohne-botschaft-a-795927.html

露呈した生体特徴を含むコンテンツを検索する、または他の同様のコンテンツと照合するために引き続き使用することができます。

VR、AR、およびメタバースに関する将来のシナリオ

トレンドマイクロは、近い将来、直接的および間接的に生体特徴を収集できる IoT（モノのインターネット）デバイスと IIoT（産業用モノのインターネット）デバイスが増加すると予想しています。仮想現実（VR）テクノロジと拡張現実（AR）テクノロジが使用され、従来のソーシャルネットワークからメタバース[19]への移行が進み、音声、動画、および生体認証の各機能が組み込まれたデバイスが日常生活の広い範囲で使用されるようになると、ユーザ情報の露呈は半永久的に続くことになります。実際、HoloLens 2（複合現実ヘッドセット）はすでに、ユーザ管理機能で虹彩認証を使用しています。同様に、他の VR プラットフォームもすでに、虹彩認識を認証に使用することを計画しています。

現在でも、動画コンテンツのアップロードをライブストリーミングと比較すると、異なる露呈のリスクが存在します。動画は見直して編集することができますが、ライブストリーミングでは機密性の高い特徴が即座に直接的に露呈します。3D オブジェクトの収集機能を備えたモバイルセンサとモバイルアプリケーションはすでに存在していますが、この収集機能には VR ユーザとメタバースユーザにとって重要な利点である顔の 3D 輪郭の収集機能が含まれています。これは、近い将来、攻撃者がより高度な顔認識テクノロジを十分に回避できるようになることを意味します。

トレンドマイクロは、今後 10 年間で大量の自動運転車が道路を走行するようになるとも予想しています。自動運転車を、カメラやセンサおよび計算機能を搭載した IIOT デバイスと考えれば、これらの自動車も生体情報の収集に最適です。生体データへのアクセスはベンダが制限する必要がありますが、それでも自動運転車の利用が増えれば、高度な攻撃者[20]がそれらのデバイスを侵害して利用する可能性があります。

マルチメディアコンテンツ処理サービスのインフラストラクチャ領域とバックエンド領域について考えることも重要です。今日、私たちは、特定個人情報（PII）と財務情報に関連するさまざまな侵害を目の当たりにしています。将来は、加工されたコンテンツではなく、生体認証データベースや、マルチメディアサービスなどのコンテンツをキャプチャして未加工の状態のままで公開するような侵害がさらに頻繁に発生すると予想されます。そのようなケースでは、プライベートまたは制限付き（特定の人とのみ共有）と考えられているメディアコンテンツも同じように露呈し、誰でもアクセスできるようになります。そのような露呈は

[19] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaworse-the-trouble-with-the-metaverse

[20] https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf

重大な影響をもたらす可能性があります。すべての生体情報について言えることですが、生体特徴が一瞬でも露呈した場合、その特徴が将来悪用されるのを抑制するのは困難です。

さまざまなサービスによるコンテンツの露呈のまとめ

これまでに説明した所見をまとめるために、コンテンツの種類と見つけることができる場所に応じて、主な生体特徴の露呈を比較する表を作成しました。コンテンツの場所には、メッセージングアプリ、ソーシャルメディアプラットフォーム、さまざまな大手ニュースサイトなどの主要ハブが含まれます。

コンテンツの種類は、音声、写真、または動画に分類しています。さらに、各プラットフォームのコンテンツで最も多く露呈している特徴の種類を強調しています。

コンテンツの場所	音声	写真	動画	状況／説明	ハッシュタグ	検索機能	よく見られるのは何か
政府／企業のポータル	中	高	中	高	低	低	😊👁〰
メッセンジャープラットフォーム	中	高	中	低	高	中	😊〰
Facebook	中	高	高	高	高	高	😊👁✋
Instagram	中	高	中	中	高	中	😊👁✋
TikTok	低	低	高	中	高	高	😊〰
YouTube	高	低	高	高	中	高	😊〰
Twitter	低	中	低	中	高	中	😊
ニュースサイト	高*	高*	高*	低	低	低	😊
設定ミス、侵害、漏えい	高	高	高	高	低	高	😊〰🫆 👁✋👂

表 1：プラットフォームおよびアプリケーションごとのコンテンツ露呈のヒートマップ

この表から、ポータルサイトの大部分は露呈レベルが中～高であること、およびいくつかの特徴、特に指紋は、大量に生体特徴を見つける簡単な方法が存在しないことがわかります。むしろ、それらの特徴が露呈する可能性があるコンテキストを考える必要があります。そう考えると、露呈を意図的、半意図的、非意図的に分類することができます。次のセクションでは、コンテキストについて詳細に調べます。

コンテンツのコンテキスト

生体データの問題の 1 つは、パスワードと異なり、一度露呈すると、変更することがほぼ不可能であることです。生体情報を意図的に露呈するケースもありますが、非意図的に露呈するほうがより危険性が高く、大規模に悪用される可能性が高まります。

意図的に露呈するもの

人が自分の行為を明確に理解した上で、指紋など、特定の特徴を露呈するケースもあります。たとえば、指紋の露呈というトピックに関する科学的な記事や動画があります。

図 13：指紋の露呈というトピックに関する動画における指紋の露呈[21]
画像クレジット：SciShow Kids/YouTube

その一方で、#Fingerprint のように直接的なタグの検索結果には、生体特徴の抽出に利用できない動画（ノイズ）が大量に含まれるので、これは大規模な生体特徴の露呈の可能性が低いと言えます。このようなケースで露呈するものは、半意図的または非意図的なものになります。

[21] https://www.youtube.com/watch?v=cZKGpg_fttw&ab_channel=SciShowKids

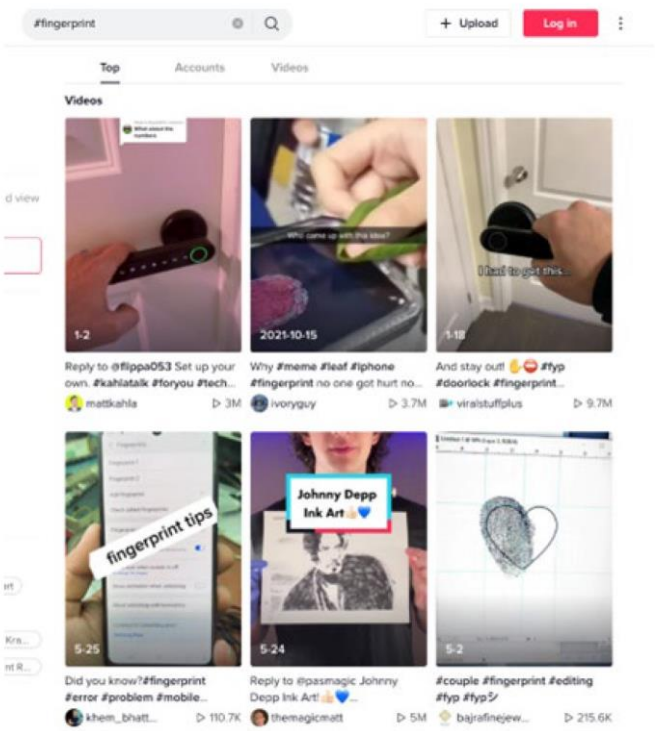


図 14：TikTok でハッシュタグ#Fingerprint を検索した結果。指紋の大量露呈につながるわけではない。

半意図的に露呈するコンテンツ

半意図的な露呈とは、コンテンツの作成者が、音声録音、または生体情報を含む身体の一部に関連する写真／動画コンテンツを公開することを意味します。そのようなケースでは、おそらく、作成者はそのような投稿が露呈につながるとは考えていません。

たとえば、高品質な肖像写真を投稿すると、顔情報が露呈します。目の写真または動画を投稿すると、高い確率で虹彩パターンも露呈します。

この種の露呈は中規模に発生します。たとえば、ソーシャルメディアには、「beautiful eyes」というフレーズのように、トレンドとなるトピックや用語があります。このフレーズを検索すると、関連するコンテンツが大量に露呈していることがわかります。

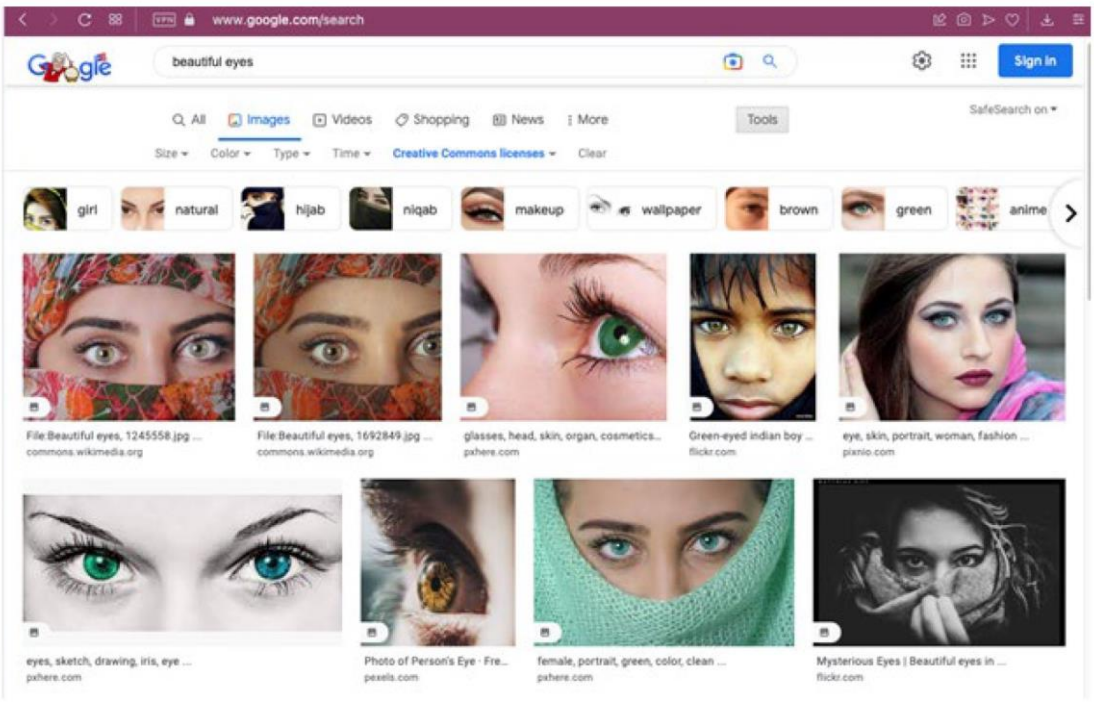


図 15：「beautiful eyes」の検索結果

非意図的に露呈するコンテンツ

非意図的に露呈するコンテンツとは、重要な生体情報が露呈しているコンテンツを指します。この場合、投稿の主なトピックは、生体特徴またはそれを露呈する身体の一部に直接は関連していません。しかし、同時に未知の露呈が発生しており、特にこのカテゴリは注意を喚起する価値があります。

次に示すワイングラスの写真はその一例です。拡大すると、ガラスに付着した指紋が露呈していることに気付きます。しかし、明らかに指紋はこの投稿のトピックではなく、露呈は非意図的です。

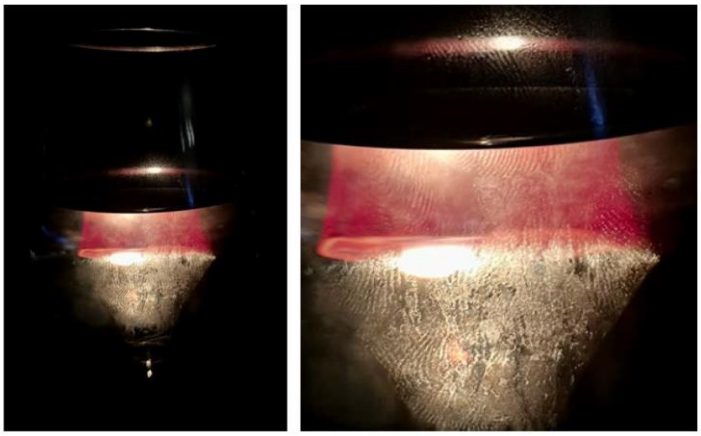


図 16：ワイングラスの写真で露呈している指紋

このようなシナリオは多数存在するので、露呈のリスクを知らなければ、そのような露呈に気付くことはほとんど不可能です。つまり、アイメイクの写真や動画について、虹彩の露呈に関連付けて考えているか、ということです。同じ疑問は、ブレスレットの写真についても当てはまります。ブレスレットの写真には、多くの場合、露呈した指紋や掌形が写っています。

Etsy の商品、結婚指輪、小さな贈り物、ハンドケア／ミニチュア料理／裁縫に関する動画などのトピックに関するメディアコンテンツは、一見すると怪しいところはありません。しかし、非意図的ではありますが、これらのコンテンツは生体情報を露呈しています。同時に、これらの写真や動画の多くは、視聴回数が数百～数千に達します。

図 17：YouTube で非意図的に指紋が露呈する例

温度などの環境変数が指紋の質に大きく影響するような物理的指紋採取と同様[22]、照明条件や機器の質も、指紋のデジタル採取に影響を与える可能性があります。収集した指紋は、犯罪現場での証拠固めに使われることもあります[23]。

[22] https://csef.usc.edu/History/2004/Projects/J0514.pdf

[23] https://researchrepository.murdoch.edu.au/id/eprint/39806/1/MacLeod2017.pdf

露呈したコンテンツを見つけるために使用したハッシュタグやピボットの例

検索対象	顔	虹彩	掌形、指紋	耳
メッセージングプラットフォーム	Makeup News	Makeup	Manicure	Haircut
Facebook	Makeup	Eye close-up	Manicure	Earings, haircut
TikTok	#Face #Makeup #MyMakeup #NoMakeup	#EyeTransition #EyeZoom #EyeChallenge #Inverted #Eyes	#HandTrend, #FingerChallenge, #MyHandsLookLikeThis #Etsy #Braslet #WeddingRing	#EarTok #Earings #EarCheck
YouTube	Interview Makeup Hairstyle News	eye zoom、eye zoom in、zoom macro、eye close up、blinking eye	Finger tattoo、 Needlework、 Miniature food	Earings
Twitter	#Hairstyle #Haircut	#Hairstyle #Haircut	#Manicure #Fingerprint	#Hairstyle #Haircut
Instagram	#Makeup #Hairstyle #Haircut	#MyEye #EyePhotography #EyePhoto #EyeyMakeup #MacroEye	#Fingers #MyHand #HandPicture #HandCloseUp #TodayOnMyhand	#Hairstyle #Haircut

表 2：各メディアプラットフォームの検索語と結果の関連性の例

表 2 は、露呈した生体情報を見つけた検索語の例です。中には、同時に 3〜5 個の生体特徴が見つかる検索語もありました。メイクアップやヘアカットに関連する動画では、顔、虹彩、掌形、および耳が同時に露呈しているものが簡単に見つかります。またニュース記事では、多くの場合、他のプラットフォームと同様に顔、掌形、および耳が露呈しています。

人々が漏えいする一般的な生体パターンはマルチメディアファイルの媒体、長さ、およびシナリオに応じて異なる

このセクションでは、単純な例として、一般的なメディアコンテンツで露呈する場合のシナリオを示します。これにより、これまでのセクションで示した情報にコンテキストを追加します。

1 番目のシナリオは記者会見です。経営幹部や政治家が歩いてステージに上がり、手を振って、聴衆に挨拶します。スピーチの間、聴衆の注意を引き付けておくために、身ぶり手ぶりを交えて、わずかに左右に体を向けます。また、定期的にコップの水を飲みます。これは、

話し手の顔、虹彩、耳、掌形、および指紋のパターンが、数分の間にすでに露呈したことを意味します。報道カメラマンやスマートフォンを持った聴衆が記者会見場にいた場合、それらの特徴が収集されたことはほぼ間違いありません。画像の品質は、機材、距離、および照明の条件によってほぼ決まります。

2 番目のシナリオでは、ミニチュア料理を作ります。この場合、作成者自身が登場して、自分の顔と、おそらく虹彩パターンを露呈します。何かを拾い上げようとすると、耳のパターンが露呈します。スプーンやフォークを持っている間は指紋が部分的に露呈し、完成した料理を見せている間は掌の情報が露呈します。

非常に短い時間で 2〜3 個の生体特徴を露呈する動画シナリオは、他にも多数存在します。たとえば、TikTok 動画は 15 秒しかありませんが、本書で説明しているほとんどすべての特徴を露呈します。

まとめると、静止写真や特徴を数秒間映す動画は機密データを露呈する可能性があるので、メディアコンテンツを公開する際はそうしたリスクを念頭に置くことが最も重要です。

生体情報のユースケース

生体情報は、長年にわたって本人確認と認証に使用されてきましたが、他の用途もあります。行動的生体情報は、人々やその習慣（運転スタイルなど）をプロファイリングするために使用されます[24]。また、ユーザコンテキストの認識にも使用できます[25]。露呈した生体データのリスクおよび考えられる攻撃パターンを理解するには、生体情報がいつ、どこで、どのように使用されるかを知ることが重要です。このセクションでは、現在および将来における生体情報の一般的なユースケースについて説明します。

自分のデバイスへのアクセス

最新のスマートフォンやタブレットの多くは、1 つ以上の生体特徴を使用して所有者を認証する機能を搭載しています。現在、最も広く使用されているのは、指紋認識と顔認識の 2 つの方法です。また、多くのノート PC も、指紋スキャナや顔認識機能を搭載しています。

生体情報は、デバイスのロックを解除するだけでなく、購入時やソフトウェアのインストール時のユーザ認証や、アプリケーションごとに内部で機密性の高い操作を実行する際の確認にも使用されています。2020 年にはスマートフォン所有者のおよそ 41%が生体情報を使用していましたが、この割合は 2024 年までにおよそ 66%にまで伸びると予測されています[26]。2020 年にはすでにスマートフォンの利用者数が 50 億人を超えていた[27]ことを考えると、20

[24] https://ieeexplore.ieee.org/abstract/document/7014406

[25] https://www.sciencedirect.com/science/article/abs/pii/S1084804516300261

[26] https://www.paymentsjournal.com/by-2024-how-many-smartphone-owners-will-use-biometrics/

[27] https://financesonline.com/number-of-smartphone-users-worldwide/

億台以上のスマートフォンで生体特徴が処理されると予測できます。こうしたデバイスへのアクセスは、今日では生体情報を日常的に使用する代表的なユースケースです。

建物の出入

建物、特に機密情報が処理される政府機関や研究機関の建物の出入は、生体情報ベースの出入管理を使用する明らかなユースケースの 1 つです[28]。物理的な出入管理で最も広く使用されているのが、指紋、顔、虹彩、および掌形の認識センサです。出入管理センサからのデータは、勤務時間を計算するため、または出入管理センサとセキュリティで保護する IT 資産（多層防御戦略を実施するために通常は建物側からのみアクセス可能）を関連付けるために使用されることがよくあります。

出入管理は、監視付きまたは監視なしで配備できます。他の方法に生体認証を組み合わせてセキュリティを強化することもできます。

学校

建物への出入を学生や教師などの許可された人だけに制限することは、学校における生体情報の明らかなユースケースです。英国では、キャッシュレスケータリング、図書館登録、コピー、ロッカーの利用、自販機、ノート PC の利用でも生体情報が使用されています[29]。

場合によっては、生体情報により、学校で政府後援プログラムが悪用されるリスクを緩和することもできます。1 つの例が、ナイジェリアで子供たちに食事を提供する NHGSFP（National Home-Grown School Feeding Programme）です。その運用の一部として、まだ食事を受け取っていない子供たちに政府資金を提供できるように、5 歳の子供の指紋と写真を収集しています。生体情報は、有効性、透明性、および説明責任を保証するのにも役立ちます[30]。

医療

医療では、患者の ID を正確に確認していることを保証するために、生体情報を使用します。リモート診断からドナーの認証、ID の同定、無意識状態で運び込まれた患者の医療記録の取得まで、幅広いユースケースがあります。

露呈した生体データが悪用される可能性として最も明らかなのは、電子処方箋システムの悪用です。

---

[28] https://documents.trendmicro.com/assets/white_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf

[29] https://defenddigitalme.org/research/state-biometrics-2022/

[30] https://guardian.ng/news/fg-embarks-on-biometric-enumeration-of-pupils-on-school-feeding-programme

銀行取引

銀行取引では、生体情報はすでに個人の認証および金融取引の確認のために広く使用されています。

- リモートとローカル、監視付きと監視なしなど、さまざまなユースケースシナリオがあります。
- 銀行が生体認証センサを管理していて、認証プロセスが適切に作動していることを銀行員が保証している場合、ローカルかつ監視付きの認証が可能です。銀行の特定の支店やオフィスにおける送金の確認は 1 つの例です。
- 生体認証対応の ATM から現金を引き出すケースもあります[31]。この場合、銀行がセンサを管理しますが、認証は監視なしで実行されます。監視なしの認証の場合、攻撃者がセキュリティメカニズムを回避するための選択肢が増えます。ATM のモデルに応じて、認証で指紋、顔認識、または虹彩認識を使用できます。ブラジルなどのいくつかの国々で設置されている ATM の中には、デビットカードやクレジットカードの代わりに、生体情報でも現金を引き出すことができます[32]。
- リモート認証を使用するが登録はローカルで行うといった場面もあります。この場合、登録は銀行のオフィスで、または信頼できるパートナーにより、監視付きで行われますが、その後の認証やリモート取引の確認には生体情報を使用します。この場面では、攻撃者は、漏えいした生体データを使用してセキュリティメカニズムを回避できます。そのためには、被害者の口座が生体認証をサポートしている必要があります。
- リモート認証を使用して登録もリモートで行うシナリオもあります。このシナリオでは、漏えいした生体データを使用して、ユーザを登録および認証できます。攻撃が成功した場合、生体情報の所有者は、銀行口座が自分の名前で開設されていることに気づかないまま、不正な金融活動に当該口座を使用される可能性があります。

重大イベント

重大イベントは、重要インフラと近い部分がありますが、こちらは存続期間が限られています。そのようなイベントでは、参加者または出席者のリスクを最小限に抑制するために、生体情報が重要な役割を果たすことができます。

たとえば、ドイツオリンピック代表団[33]は、その施設に不正な人物が出入するのを制限するために、生体情報ベースの出入管理を使用しました。スポーツイベントへの出入を許可するために、ID の確認とワクチン接種状況のチェックも組み合わせました[34]。

---

[31] https://ieeexplore.ieee.org/document/8605473/authors#authors

[32] https://www.marketplace.org/2013/08/06/brazilian-banks-lead-way-biometrics

[33] https://www.zdnet.com/article/programming-languages-its-time-to-stop-using-c-and-c-for-new-projects-says-microsoft-azure-cto

[34] https://www.sportsbusinessjournal.com/Journal/Issues/2022/07/11/Portfolio/Facilities-and-Ticketing.aspx

ClearのHealth Passがユーザのワクチン接種状況を証明する方法を提供
提供：CLEAR

図 18：スポーツイベントへの入場を許可する前に ID を確認し、ワクチン接種状況をチェックするアプリ
画像クレジット：Clear application

国境検問所および空港警備

国際国境検問所および空港警備で生体情報が使用されることが増えています。出入国管理の手続き中に頻繁に指紋と顔の記録と確認が行われるなど、さまざまなユースケースがあります。

こうした手続きでは、一般的な旅行者の行動に基づいて、カスタマイズされたセンサとフル HD の Web カメラの両方が使用されます。これは、機材の品質またはコストに応じて、攻撃対象領域が拡大または縮小することを意味します。実際、主要なハブ空港では、担当者と対面してやり取りする必要のない国境検問所オプションがすでに導入されています。国境検問所に加えて、一部の空港ではすでに生体情報ベースのチェックインプロセスと搭乗プロセスを使用しています。フランクフルト、ウィーン、ミュンヘン、およびハンブルクでは、スターアライアンスのフライトで顔認識搭乗プロセスを使用しています[35]。

パンデミックとマスクの必要性により、虹彩ベースの認証は、最も好まれる認証方法の 1 つになっています。空港やイベントでの認証機能を提供している、Clear などのサービスプロバイダは、現在、世界的に公衆衛生対策が実施された結果として目のみの認証を可能にしています[36]。

国民デジタル ID および法執行機関の生体情報データベース

法執行機関は、長年にわたって、捜査で IAFIS（Integrated Automated Fingerprint Identification System）などの指紋データベースを使用していました。現在の動向として、

[35] https://www.lufthansagroup.com/en/newsroom/releases/contactless-travel-with-facial-recognition-star-alliance-biometrics-now-also-at-hamburg-airport.html

[36] https://www.biometricupdate.com/202201/easier-queues-with-biometrics-touchless-check-ins-set-to-reach-more-airports

顔、指紋、虹彩など様々な生体特徴に基づいて ID を照会できるように、さまざまな種類の生体特徴をそれらのデータベースに統合しています[37]。

多くの国で、法執行機関のデータベースと共に、国民デジタル ID および国民生体情報登録が導入されています。これは、政府機関や営利団体が、本人確認と認証にそれらの一元化されたデータバンクを使用できることを意味します。これらのデータバンクは、行政、金融、および医療の各サービスに統合されることが多く、銀行、フィンテック、通信事業、IT サービスなど、数百の政府部門や民間部門のサービスの本人確認と認証に使用できます。このようなプログラムは、インドの Aadhaar Card[38]プロジェクト、UAE Pass[39]など、多数導入されています。

将来のユースケース

近い将来、次に示す要因により、生体情報が果たす役割はさらに重要になります。

- 生体認証センサまたは生体認証機能を搭載したデバイスの数が増加しています。今日出荷される新しいモバイルデバイスの 80%以上が生体認証機能を搭載しています[40]。
- 現在、特に顔認識で使用できるアルゴリズム[41]と API[42]が増加しています。
- 大手企業が、その製品とサービスで生体情報のネイティブなサポートを開始しています。
- YouTube のような大手メディアサービスのサービス利用規約に顔認識を明示的に含むコンテンツへの制限が追記されていることは、生体情報の重要性が高まっていることを間接的に示しています。同時に、これらの更新で生体データの収集が制限される可能性はありますが、メディアコンテンツから抽出できる生体特徴は他にもまだ多数存在します。

[37] https://www.biometricupdate.com/202201/easier-queues-with-biometrics-touchless-check-ins-set-to-reach-more-airports

[38] https://uidai.gov.in/en/about-uidai.html

[39] https://icp.gov.ae/en/uae-pass

[40] https://identityweek.net/evolution-not-revolution-why-mobile-fingerprint-sensors-are-here-to-stay

[41] https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/quickstarts-sdk/identity-client-library?tabs=visual-studio&pivots=programming-language-csharp

[42] https://docs.aws.amazon.com/rekognition/latest/dg/faces.html

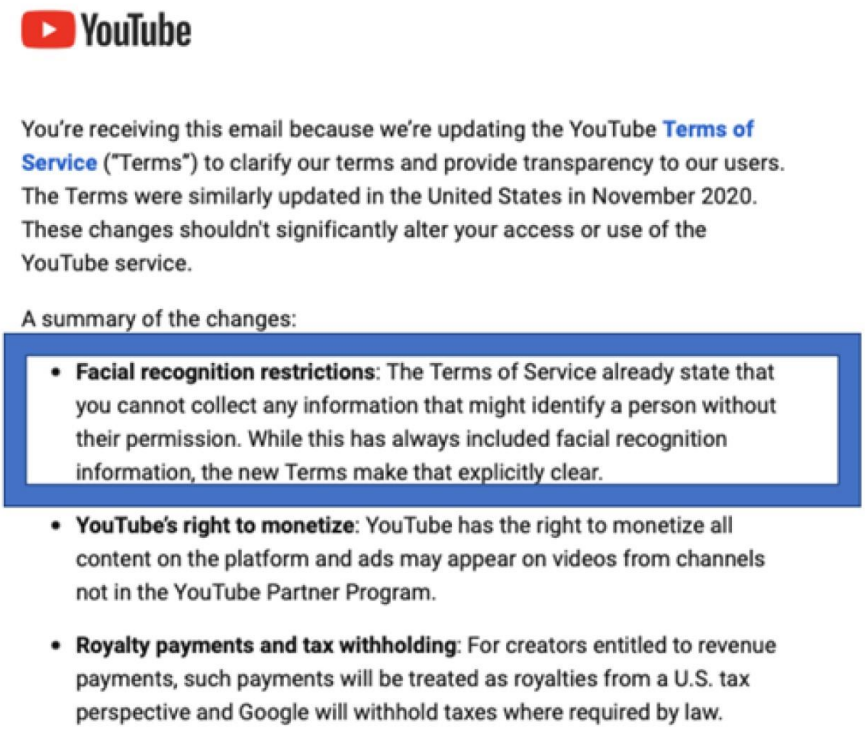


図 19：YouTube はサービス利用規約を更新して、米国において明らかな顔認識が含まれるコンテンツを制限した。この更新は、米国内では 2020 年 11 月に、米国外では 2021 年 6 月に実施された[43]
画像クレジット：YouTube Help/Google

生体情報が重要な役割を果たすさまざまなシナリオが、今後出現することが予想されています。その中には、概念実証されているものや、次世代小売業など、すでに展開されているものもあります[44]。将来、これらのテクノロジが他の国や地域に拡大することが予想されています。

次世代店舗および公共交通における非接触型透過決済

次世代小売業[45]の概念では、スマートシェルフ、広範囲にわたるロボット技術の利用、現金やクレジットカードを必要としない決済手段などのさまざまな機能を、その重要な特徴として考えています。小売業者が提供する専用アプリを店舗入口で使用することによって、QR コードを生成する場合もあります。また、プロセスの透明性をさらに高めて、生体情報を登録済みの顧客を店内で自動的に認識して追跡する場合もあります。顧客が店舗を出るときに

[43] https://support.google.com/youtube/answer/10090902?hl=en#zippy=%2Cwhy-did-you-change-the-terms-of-service%2Cwhat-are-the-main-changes%2Chow-will-this-affect-my-ypp-monetization%2Cdoes-this-have-to-do-with-the-european-union-copyright-directive-or-gdpr%2Cwhat-does-this-mean-for-my-privacy-or-data

[44] https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain

[45] https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain

決済を開始する際は、生体特徴も使用します。したがって、このテクノロジは、使いやすさだけでなく、追跡することに対する懸念ももたらします[46]。

同様のユースケースとして、生体情報を使用する公共交通の透過決済があります。このテクノロジは、近年、モスクワ[47]、ドバイ[48]などの巨大都市で使用できるようになっています。

国勢調査、投票、および選挙

国連は 2002 年のシンポジウムで、人口調査等の国勢調査において、他のイノベーションと共に生体認証テクノロジを使用することについて議論しました[49]。

現在、生体認証有権者システムを導入する国がますます増えています。このような状況において、認証情報を共有することで同時に複数の人の代理投票が可能になってしまう事態を避けるために、生体情報が重要な役割を担っています[50]。実際、生体認証投票システムによって異常が検出された事例がすでに確認されています。ナイジェリアでは、二重登録を含む無効な登録が 100 万件以上検出されました[51]。

インターネット上の投票や申請に関しては、結果を操作するさまざまな攻撃手法が存在します[52]。近い将来、生体認証テクノロジにより、インターネット上の投票や申請の完全性が大幅に向上する可能性があります。

社会信用システム

社会信用システムはすでに中国で利用されていますが、今でも盛んに開発が続けられています[53]。同様のシステムを稼働する技術的能力を備えている国は他にも多数存在しますが、ヨーロッパでは国家レベルでこのようなシステムを導入することについて、プライバシー上の懸念が多数指摘されています。保険[54]などの一部の業界や法執行機関[55]では、これらのテク

[46] https://www.forbes.com/sites/forbesbusinesscouncil/2020/05/08/how-facial-recognition-will-change-retail/?sh=3db4b94f3daa

[47] https://techxplore.com/news/2021-10-moscow-metro-recognition-payments.html

[48] https://techxplore.com/news/2020-10-dubai-facial-recognition.html

[49] https://unstats.un.org/unsd/demographic/docs/symposium_06.htm

[50] https://thewire.in/government/election-commission-says-it-is-time-to-exlore-remote-voting

[51] https://www.biometricupdate.com/202204/nigerias-biometric-voter-system-detects-over-1m-invalid-entries

[52] https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf

[53] https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020

[54] https://www.marketwatch.com/story/should-you-let-your-car-insurer-monitor-you-2019-03-27

[55] https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras

ノロジがすでに導入されています。近いうちに、これらの社会信用システムの結果を何らかの形で使用する業界が増えることが予想されます。

生体情報、特に顔認識は、このプロセスで重要な役割を果たします。全体的に見て、通信テクノロジが 5G から 6G に移行すると、人々の行動や習慣を追跡する機能が大幅に向上することが予想されます。なぜなら、人間の行動を追跡できるセンサの数と種類が増加するからです。

AI システムが、バスの車体広告のモデルの顔を、道路で信号無視している人間だと誤認識した事例がすでに知られています。この誤認識は社会信用システム内でのそのモデルの評価に自動反映されてしまい、後日手作業で修正されるまでその影響は残っていました[56]。

[56] https://www.bbc.com/news/technology-46357004

人々に及ぼす影響：現在と将来の攻撃シナリオ

このセクションでは、現在と将来の攻撃シナリオについて説明します。現在の攻撃シナリオは、簡単かつ大規模に実装できるものです。将来の攻撃シナリオには、すでに使用可能だけれども大規模に使用されていないテクノロジを使用するシナリオや、テクノロジのプロトタイプや概念実証はすでに存在していて将来攻撃を行う者が出現することが予想されるシナリオが含まれます。

このセクションの目的は、生体特徴が露呈した後に生じる可能性があるリスクについて認識を広めることです。

攻撃シナリオ		顔		指紋		虹彩	
		現在	将来	現在	将来	現在	将来
生体情報の収集	生体情報の受動的な収集	高	高	低	中	低	高
	生体情報の能動的な収集	高	高	中	高	中	高
ID窃盗およびなりすましによる攻撃	ディープフェイク	高	高	低	低	低	高
	スマートデバイスの悪用	低	高	低	低	低	中
	テクニカルサポートをだますことによるアカウント乗っ取り	中	高	低	中	低	中
	人物の存在の捏造	低	高	低	中	低	中
	社会信用システムの侵害	低	高	低	低	低	中
IDを使用する攻撃	人物とその習慣の追跡と自動識別	高	高	低	低	低	中
	人々がやり取りするコミュニティの特定	高	高	低	低	低	中
	恐喝しやすい状況の創出	高	高	中	高	低	中
	重大イベントに出席する人物の特定	高	高	低	低	低	低

攻撃シナリオ		顔		指紋		虹彩	
		現在	将来	現在	将来	現在	将来
認証への攻撃	ノートPCや携帯電話などの機器のロック解除	高	高	高	高	低	高
	次世代小売業、公共交通決済、および現金引き出し	高	高	中	高	低	高
	生体認証機器による口座取引や金融取引の確認	高	高	中	高	低	高
	将来のデバイス	低	高	低	中	低	高

攻撃シナリオ		声		掌形		耳	
		現在	将来	現在	将来	現在	将来
生体情報の収集	生体情報の受動的な収集	高	高	低	中	低	低
	生体情報の能動的な収集	高	高	低	中	低	低
ID窃盗およびなりすましによる攻撃	ディープフェイク	高	高	低	中		
	スマートデバイスの悪用	高	高	低	中	低	低
	テクニカルサポートをだますことによるアカウント乗っ取り	高	高	低	低	低	低
	人物の存在の捏造	低	高	低	低	低	低
	社会信用システムの侵害	低	中	低	低	低	低
IDを使用する攻撃	人物とその習慣の追跡と自動識別	中	高	低	低	低	低
	人々がやり取りするコミュニティの特定	中	高	低	低	低	低
	恐喝しやすい状況の創出	低	中	低	低	低	低
	重大イベントに出席する人物の特定	低	中	低	低	低	低

攻撃シナリオ		声		掌形		耳	
		現在	将来	現在	将来	現在	将来
認証への攻撃	ノートPCや携帯電話などの機器のロック解除	低	低	低	低	低	低
	次世代小売業、公共交通決済、および現金引き出し	低	中	低	低	低	低
	生体認証機器による口座取引や金融取引の確認	低	中	低	低	低	低
	将来のデバイス	低	中	低	低	低	低

表 3：攻撃シナリオごとの生体特徴の使用方法および現在と予想される将来の使用方法の比較のヒートマップ

生体データの収集とそれと連携した攻撃

攻撃者は、生体特徴を使用するために、それらを収集または傍受する必要があります。特徴の収集は受動的または能動的に行われます。受動的な収集とは、特徴の所有者または生体データを保管または処理する組織が気付かない方法で収集することを意味します。能動的な収集とは、特徴の所有者または生体データを保管または処理する組織が気付く方法で収集することを意味します。

生体データの受動的な収集

受動的な収集は、本書でこれまで説明した公に露呈した特徴に関連する場合がほとんどです。そのような情報の主な供給源は、ソーシャルメディアネットワーク、メッセージングプラットフォームネットワーク、ニュースサイト、および政府と企業の公式ポータルです。FindFace[57]は、人を顔パターンに基づいて特定するためにソーシャルメディアネットワークである vk[.]com の写真を大量に処理するサービスの 1 つです。

生体データの能動的な収集

生体情報の能動的な収集とは、生体特徴の収集を目的とした攻撃を意味します。注目すべきは、受動的収集が可能な場合はそのような能動的行為は不要だということです。本書の主な焦点である、ソーシャルメディアにおける生体情報の受動的な漏えいに加えて、攻撃者が能動的に使用できる生体データの供給源を示すことにもまた意義があります。

このセクションでは、生体データの能動的な収集に関連するさまざまな攻撃シナリオについて 1 つずつ説明します。

生体認証エコシステムへの攻撃

生体認証エコシステムの最も単純なケースシナリオは、スタンドアロン実装、つまりセンサまたはセンサに直接接続されているホストにパターン情報を保管する実装です。この実装は、ジムの出入口のような 1 つの資産の利用を 1 つの生体認証センサで管理するようなスモールオフィス（SOHO）や中小企業（SMB）に関連して多く行われています。

分散して配置された複数のセンサを接続する実装には、もっと複雑なアーキテクチャを使用する必要があります。この実装には、多くの場合、生体認証センサ、クラウドまたは集中型のデータベース、およびさまざまな認証サービスとの統合 API が含まれます。これらのコンポーネントはすべて、設定ミス、悪用可能な脆弱性、または内部的な脅威が存在する場合、生体パターンの抽出に利用される可能性があります。生体認証サービスを提供するサードパーティベンダは、ビジネスプロセスで機密性の高い個人、政府、または企業のデータや情報を有していることが多いので、潜在的に攻撃者に利益をもたらす可能性の高い標的であり、サプライチェーン攻撃における重要な拠点としても捉えられます。

センサへの攻撃

センサ（通常の携帯電話ではない、ハードウェアの生体認証センサ）は、攻撃者によって設置、制御、または変更される可能性があります。このシナリオにおける攻撃は、センサ出力を傍受できるようにする ATM へのスキマー攻撃(キャッシュカードなどの磁気記録情報を盗む手口)に似ています。多くの場合、これらの攻撃は簡単に実装できます。

[57] https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/?sh=5c154311463b

たとえば、ATM にカメラや指紋スキャナが追加されても、驚く人はほとんどいません。これは、現在多くの店舗で非接触型決済デバイスが置かれている状況に似ています。しかし、攻撃者は、現金や決済の管理に使用される装置または資格情報を侵害できます。

ソフトウェアサプライチェーンも、特にサードパーティ製のライブラリ、API、またはソフトウェア開発キット（SDK）を使用している場合は、さまざまな場所で破壊される可能性があります[58]。他の業界でも、タクシー運転手向けに、GPS データを改ざんして実際より長い距離の料金を乗客に請求する改造アプリケーションを地下犯罪組織が販売するなどの前例があります[59]。簡単に言うと、そのような攻撃に必要なすべてのテクノロジはすでに確立されており、広い範囲で問題が認識されるのは時間の問題でしかありません。

データベースへの攻撃

今日、データ侵害は定期的に発生しています。侵害により PII が露呈したというニュースを頻繁に耳にしますが、生体データを露呈する設定ミスなどのインシデントも同様に発生していることは注目に値します[60, 61]。また、本来は侵害があったことは公表される傾向がありますが、中には攻撃者が誰にも気付かれずに生体データをサポートするデータベースやバックエンドのインフラ設備を侵害できたために公表されていないケースもあるでしょう。

API およびエクスポート機能の悪用

多数の生体認証エコシステム（特に分散型エコシステム）に対して相互運用性を提供するには、パターン情報または収集した未加工の生体特徴をエクスポートする機能が必要です。この機能は、通常は、コンプライアンス要件に含まれています。データ交換形式は標準化されており、生体データ交換形式を定めた ISO/IEC 19794 シリーズや ANSI/NIST-ITL 1 はそのような標準の一例です。攻撃者は、そのようなデータ交換機能を悪用して、システムに登録されているアカウントに関連する生体データを取得できます。

生体認証関連の API も、生体パターンまたはセンサが収集した未加工データを抽出するのに使用できます。このことは、近年発表された研究でも確認されています。たとえば、Android の指紋 API の使用方法に関するレポート[62]は、生体情報関連の Android API のセキュリティ問題を取り上げています。一部の Android ベースのデバイスにも、API 経由の生体

[58] https://www.first.org/conference/2022/program#pYour-Phone-is-Not-Your-Phone-A-Dive-Into-SMS-PVA-Fraud

[59] https://www.trendmicro.com/vinfo/ae/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars

[60] Patrick Howell O'Neill. (Aug. 14, 2019). *MIT Technology Review*. "Data leak exposes unchangeable biometric data of over 1 million people." Accessed on Sept. 23, 2022

[61] https://www.safetydetectives.com/blog/antheus-leak-report

[62] https://reyammer.io/publications/2018_ndss_fingerprint.pdf

特徴情報の抽出に関する脆弱性があります。携帯電話から指紋を抽出できる API の脆弱性に関するレポートも発表されています[63]。

分散型生体認証システム関連の API も悪用される可能性があります[64]。この API は、既存のインフラストラクチャにアクセスする手段を収益化する方法を犯罪者に提供します[65]。たとえば、侵害された組織がいくつかのプロセスに生体情報の本人確認と認証を統合した場合、犯罪者はアクセスする手段を悪用して不正に利益を得ることができます。

相互運用性があるがゆえに、収集したデータは、ユーザの許可を得ずに他の生体認証システムにインポートされる場合や、侵害済みのセンサまたは攻撃者が管理するセンサの代わりにシステムに情報として注入される場合ができます。

未加工データおよび生体特徴を抽出するメディア処理アルゴリズムへの攻撃

インターネット接続は世界規模なので、特にメディアコンテンツが暗号化されていない場合または安全でない接続を使用してストリーミング、ダウンロード、またはアップロードされる場合は、メディアサービスに関連するサプライチェーン全体を管理するのは困難です。また、メディアの電波は、複数の司法管轄区域にまたがって送信されている可能性があります。これは、いずれかの中間地点でメディア処理アルゴリズムが導入され、私たちの管理が及ばない状況で生体情報が抽出および処理される可能性があることを意味します。

生体情報を抽出する監視システムへの攻撃

監視システムは生体特徴（主に顔の画像）を収集するための金鉱ですが、場合によっては声、掌形、および耳のパターン情報も含まれる可能性があります。中国[66]とロシア[67]の両国ではすでに顔認識を使用するシステムが中央集権的に管理されており、これが実現しています。

他の場所でも、同じ装置を使用して生体パターンを収集することは可能です。監視システムが公に露呈しているケースは多数存在しており、これらのシステムは場所やコンテンツの種類で分類されています。トレンドマイクロは以前の調査で、確立されたビジネスモデルの一部として、アンダーグラウンド市場において監視システムへのアクセス手段が販売されていることについて説明しました[68]。

---

[63] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7958

[64] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1022.5453&rep=rep1&type=pdf

[65] https://www.trendmicro.com/de_de/research/20/i/the-life-cycle-of-a-compromised-cloud-server.html

[66] https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08

[67] https://www.themoscowtimes.com/2018/05/24/russias-gazprom-satisfied-after-settling-eu-antitrust-case-without-fines-a61566

[68] https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras

ID 窃盗およびなりすましによる攻撃

デジタル ID はすでに、私たちの生活の中で重要な役割を果たしています。一部の国では、アプリケーションのロックを解除または取引を認証するために生体情報を登録する必要がある SIM カードまたはモバイルアプリに、個人のデジタル ID がリンクされています。これは通常、一般的によくあるプラスチックなどに印刷されている物理 ID とデジタル ID の間に信頼された関係を確立する手続きが存在し、信頼関係が確立した後は従来の ID を物理的に提示しなくてもデジタル ID を使用すればさまざまな活動を実行できることを意味します。

信頼できる関係を確立する段階からは、この種の新しい ID の侵害、乗っ取り、またはクローンの作成が、実生活で重大な結果を招く恐れがあります。中でも特に、政府のポータルサイトのアカウントまたは金融機関関連のアカウントを含むアカウントの乗っ取りは起こり得るでしょう。攻撃者は、アカウントを使用して、特定の状況で特定の場所にその人物がいたことを装う証拠を捏造することもできます。

ディープフェイク

ディープフェイクは、国または特定の業界に対して影響力を持つ人々の評判に、深刻なダメージを与えることができます。これは、著名人が自動的に標的になる可能性があることを意味します。さらに重要なのは、こうした人々はほぼ間違いなく、その静的にも動的にも生体特徴をすでにメディアコンテンツ経由で大々的に露呈しているという点です。残念ながら、この露呈を使用してディープフェイクモデルをトレーニングすることができ、すでにたびたび政治家がその被害に遭っています[69, 70]。

この活動がさらに大規模に行われた場合、犯罪者はすでに CEO のディープフェイクを使用して民間企業を標的とするテクノロジを採用しているので、生体特徴または生体資産の所有者に対して重大な影響を及ぼす可能性があります[71]。トレンドマイクロは以前、欧州警察組織および国連地域間犯罪司法研究所（UNICRI）との共同研究で、この件について詳しく調査しました[72]。

ディープフェイクにより、金融機関のセキュリティメカニズム、特に動画による動的な生体情報認証を回避できる方法を示す概念実証が存在します[73]。しかし、ここで重要なリスクは、サイバー犯罪者や国家が支援するグループもそれらのテクノロジを使用する可能性があるという点です。

---

[69] https://ars.electronica.art/center/en/obama-deep-fake

[70] https://www.bbc.com/news/av/technology-50381728

[71] https://www.business-standard.com/article/news-ani/deepfake-ceos-are-stealing-millions-from-companies-119071901535_1.html

[72] https://www.trendmicro.com/vinfo/ie/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml

[73] https://www.paymentvillage.org/blog/how-i-used-deepfakes-to-bypass-security-verifications-in-a-bank

ディープフェイクテクノロジによる金銭窃取

近年、アンダーグラウンド市場におけるフォーラムでは、金融詐欺などの悪意のある活動にディープフェイクを使用することが議論されています。さまざまなサイバー攻撃の成功率と収益率を大幅に向上させることができるテクノロジは、予想どおり、登場して間もないころからアンダーグラウンドユーザーの関心を集めていました[74]。ディープフェイクは、ビジネスメール詐欺（BEC）、メッセージング詐欺、テクニカルサポート詐欺、マネーロンダリング用アカウントの作成、金融機関のアカウント乗っ取りなど、既存の攻撃に大変革をもたらし、強化することができます。

重大イベントでのディープフェイクによる攻撃

ディープフェイクを使用して、国の指導者や政府代表者を模倣して不適切なタイミングで重要な発言をさせるようなシナリオは、深刻な結果をもたらす可能性があります。たとえば、フリーのジャーナリストが少ない国の政府代表者のディープフェイクが、損害を与えかねない発言をした場合、国内で重大な事態を引き起こす、外交活動に影響を及ぼす、あるいは株式市場に影響を残すといった可能性があります。したがって、重要な場面では、こうした捏造の影響はかなり大きくなる可能性があります。

より具体的な例として、ディープフェイク動画により、特定の材料、テクノロジ、または商品の輸出が保留される場合があります。当該国の市場シェアが大きいか、ほぼ独占的である場合、そのような発言が多くの地域に影響を及ぼす可能性があります。

ディープフェイクには、特定の地域または特定の社会集団に騒動を引き起こす、または騒動を拡大する潜在的能力もあります。

スマートデバイスの悪用

公開されているメディアコンテンツを使用して、スマートスピーカーや音声アシスタントをだまして悪用することができます。これらのデバイスは、複製された音声メッセージまたは近くにあるデバイスで再生されたメッセージに基づいてコマンドを受け取る[75]ことができます。大きな害の無いいたずらでこうした攻撃方法が使用される可能性もありますが、一部のスマートホームデバイスは買い物を行うこともできるので、そのようなデバイスの所有者にはこの攻撃が経済的な影響を及ぼす可能性があります。このことは、音声認識で認証を行うデバイスに固有のリスクがあることを示しています。

テクニカルサポートをだますことによるアカウント乗っ取り

テクニカルサポートに電話すると、いわゆる本人確認（KYC）プロセスがアカウントを回復するために何らかのメディアコンテンツを要求する場合があります。たとえば、露呈しているメディアを再利用できる特定の位置で自撮りを要求したり、通話中に自撮りを要求したり

[74] https://www.paymentvillage.org/blog/how-i-used-deepfakes-to-bypass-security-verifications-in-a-bank
[75] https://documents.trendmicro.com/assets/pdf/the-sound-of-a-targeted-attack.pdf

します。ただし、最新の機器は動画または音声のストリームにリアルタイムに適用できるフィルタを作成できるので、漏えいした生体情報を攻撃者が事前に収集し、それに基づいて標的の外観または声を模倣することができます。

攻撃者は同じ戦略を適用して、コールセンター経由で提供されるサービスを標的にすることができます。このシナリオでは、攻撃者は、リアルタイムに音声生体情報を使用します。この種のテクノロジは 10 年以上前から利用されており、金融機関で多く使用されている点に注意する必要があります[76]。

特定の場所またはイベントに人物がいたことにする捏造

特定の場所またはイベントに人物がいたことを捏造するシナリオがあります。たとえば、攻撃者は、顔識別機能を搭載した監視システムでその人物に一致する人がいたという事実を発生させることや、露呈しているメディアコンテンツから収集した生体特徴を使用して生体情報ベースの決済取引（公共交通など）を実行することができます。

攻撃に選ばれた場所またはその周辺の機密性に応じて、これらの悪意のある活動が生体特徴の所有者に現実世界で重大な結果をもたらす可能性があります。実際に結果が目に見える単純で明らかなシナリオが存在します。

説明のために、生体情報を使用するカーシェアリングサービスアプリの例を取り上げます。攻撃者がユーザの生体情報の悪用に成功した場合、アカウントを認証し、さらにユーザの名前で車両を盗むことができます。生体情報の所有者はおそらく捜査対象となり、罪を着せられるでしょう。今日、生体認証オプションを利用できるカーシェアリングアプリはますます増えており、この状況が発生しやすくなっていると繰り返し伝えることは意味があると言えるでしょう。トレンドマイクロは、以前発表した論文で、携帯電話に関連付けられた盗難 ID を使用する同じようなシナリオについて説明しました[77]。

考えられる別のシナリオとして、攻撃者が、不審な場所に人物がいたことを捏造する偽の証拠を仕込む可能性があります。このシナリオでは、犯罪グループが特定の場所に集まることを知っている攻撃者が、犯罪現場で監視システムを起動し、それと同時に攻撃対象者の生体データに関連付けられているアカウントを使用して既知のマネーロンダリング口座に送金できます。基本的に、攻撃者は、生体データを使用して対象者の不審な行動を捏造することができます。

これらの行動は、法執行機関の捜査、身元調査、および報道記事につながる可能性があり、これらはすべて生体情報の所有者の評判に影響を及ぼす可能性があります。

---

[76] https://www.biometricupdate.com/201205/bank-call-centers-using-voice-verification

[77] https://documents.trendmicro.com/assets/white_papers/wp-sms-pva-underground-service-enabling-threat-actors-to-register-bulk-fake-accounts.pdf

なりすまし攻撃による評判の侵害

露呈した生体情報を使用したなりすまし攻撃により、人物の評判に影響を及ぼすことができます。その目的は、恐喝、詐欺、政治的利益、企業の利益などが考えられます。攻撃者は、写真、音声、動画を使用して、それらに別の説明を付けて投稿したり、別の時間に投稿したり、別のコンテキストを付加して投稿したりできます。また、恐喝や詐欺を目的として、親戚や友人にメッセージングプラットフォームで音声メッセージを送ることもできます。

ソーシャルメディアネットワークにおける生体情報ベースの本人確認[78]と認証[79]に関連して、ますます多くの開発が行われています。これは、以前トレンドマイクロが発表した論文に対応付けることができます。この論文では、攻撃者が生体認証センサと処理アルゴリズムを回避し、特定のソーシャルメディアアプリまたはソーシャルメディアアカウントを使用してデバイスへのアクセスを取得できる方法について説明しています[80]。このケースでは、攻撃者は、生体データの所有者の評判に悪影響を与える可能性のある投稿、コメント、エンゲージメント、またはグループへの参加を開始できます。

社会信用システムの侵害

社会信用システムは、国全体で、または特定の業界に限定して実施できます。公共の場所またはデジタル世界で特定の人物になりすます機能は、その人物の司法管轄区域に社会信用システムが導入されている場合に、人物の生活に大きく影響を及ぼす可能性があります。たとえば、自動車保険料は、保険をかける人物の運転習慣に大きく依存する可能性があります[81]。これは、そのような人物になりすます、またはそのような人物にリンクされているデジタル ID になりすますだけでも、保険料だけでなく、その人物の生活の多くの側面に大きな影響を及ぼす可能性があることを意味します。

都市監視システムの起動するような場合、具体的には、ウイルスが大発生してその後ロックダウンが行われた場合や違法な街頭抗議が行われた場合に、起動したシステムによって金銭の請求または刑事告訴の対象になる可能性があります。一部の人にとっては、これがキャリアの破綻を意味する可能性もあります。

近い将来、攻撃者が利用できる、評判システムと社会信用システムの両方を標的とする方法がますます増えることが予想されます。さらに、生体データを含むメディアコンテンツが露呈した場合は、そのような攻撃を実施するためのコストが下がることも予想されます。

---

[78] https://abcnews.go.com/Technology/wireStory/instagram-tests-ai-tools-age-verification-85592466

[79] http://article.nadiapub.com/IJSIA/vol8_no6/5.pdf

[80] https://documents.trendmicro.com/assets/white_papers/wp-sms-pva-underground-service-enabling-threat-actors-to-register-bulk-fake-accounts.pdf

[81] https://time.com/nextadvisor/insurance/car/telematics-monitor-driving-insurance-discount

ID による攻撃

生体特徴が、特に地理位置情報と一緒に、大規模に露呈した場合、人々の活動を大規模に追跡する機会となってしまいます。そのような攻撃では、露呈規模と認識対象の範囲が大きいので、基本的には顔情報を用いた個人の識別が行われる可能性が最も高いですが、音声情報を使用できる場合もあります。

個人の特定に関してはさまざまな攻撃が存在します。このセクションではプライバシー関連のシナリオを取り上げます。

人物とその習慣の追跡と自動 ID 判別

顔が実名と一緒に露呈している場合、顔認識機能を備えた監視カメラをトレーニングするためのトレーニングデータセットとして利用できます。政府、金融機関、民間企業（通常は生体特徴の収集について書面による同意が必要）はこのトレーニングを実行できますが、この種のデータにアクセスできる攻撃者も同様にこのトレーニングを実行できます。

一連のカメラにアクセスできる攻撃者は、特定の日時における人物の詳細な位置を追跡できるデータを取得できます。メディアコンテンツで背景環境を特定することにより、人物の習慣や弱点を追跡することもできます。このデータは、脅迫、個人を狙ったフィッシングメールの準備、評判に対する攻撃、世論の操作などの攻撃シナリオで使用できます。ある人物の食べ物の好みや特定のトピックに関するイベントへの参加に熱心であることを知った攻撃者がそのような情報を使用した場合、その人物へのフィッシング攻撃の成功確率を大幅に向上させることができます。近い将来、特に 5G から 6G へ移行する際に、センサの接続性が高まることを考えると、それらのセンサが収集したデータを使用して、より正確に位置や習慣を追跡することもできるようになります。また、新しいテクノロジが登場するたびに繰り返されることですが、今までのところ、法的要件は非常に限定されているので、接続性に関連するリスクが増えることも強調する必要があります。通常、新しいテクノロジが悪用されてから法的規制が形になるまで数年のギャップがあり、いわば「西部開拓時代」のような期間があります。

現在、ソーシャルメディアネットワークで露呈しているデータでトレーニングした顔や感情の認識モデルを販売する新しい企業がすでに登場しています。また、習慣に関するデータは一般には匿名化されていると考えられていますが、ソーシャルメディアでは最近書き込んだ内容に関連する非常に精度の高い広告が表示されます。このデータを組み合わせることで、攻撃者は、商業スパムから国家的な企みまで、さまざまな心理作戦で使用できる正確で強力な資源を得られます。

人々がやり取りするコミュニティの特定

グループで撮影した写真や動画の顔を認識し、各自の職業を含むソーシャルメディアプロフィールに対応付けることで、雇用主、地位、場所、イベントの日時などの多数のパラメータ

を特定できます。今日、さまざまなオンラインサービスが、顔からその他の情報を取得するこの種の正確な画像検索機能を無料または有料で提供しています。

特定の日時または特定のコンテキストで物議をかもす人物と一緒に登場することも、人物の評判や政治生命にまでも大きな影響を及ぼす可能性があります。そのように登場したことが、適切なタイミングで適切な聴衆に適切な範囲で提示された場合、大きなダメージを与える可能性があります。このシナリオは、政治家が飲酒による問題を起こして辞任を迫られることや隔離期間中に有名人の集まりに参加したことを謝罪することにつながる可能性があります。どちらも現実的なシナリオであり、すでに最近のニュースでそのような話題が取り上げられています。

露呈したデータに基づく恐喝しやすい状況の創出または世論の操作

今日、動画や写真は、最初に公開されたときの状況とは別のイベントに関連付けられて公開される

可能性があります。この種のメディアは、視聴者の印象を大きく変える可能性があります。

たとえば、数年前に軍事訓練を受けた人物を特定する動画が公開されて、あたかもその人物が現在進行中の軍事活動に積極的に関与しているように見えるとします。そのような投稿は、本人がそのことを認識して行動を起こす前に、簡単にニュースサイトに掲載される可能性があります。公開されたことが、イメージが大きく悪化すること、進行中の交渉が影響を受けること、または複数の国家間で深刻な緊張が生じることにつながる可能性があります。

残念ながら、そのような悪意のある活動の長期的な影響は否定されたとしても、短期的な衝撃だけで、攻撃者が望んだとおりのダメージがすべて実現します。露呈した生体情報は、いわゆる人肉検索（HFS）[82]を強化し、そのような攻撃の被害者に与えるダメージを増やす可能性があります。

重大イベントに出席する人物の特定

重大イベントとは、通常のイベントに比べてインシデントのリスクや影響が大きい、公的または私的な期間限定のイベントです。例として、オリンピックやワールドカップなどのスポーツイベント、選挙などの政治イベント、大統領または首相が出席する会議、演説会、ストライキ、自然災害などがあります。このようなイベントに参加している人物がメディアで露呈した場合、肯定的結果と否定的結果の両方がもたらされる可能性があります。

一方、個人レベルでは、困った状況や恐喝される事態をもたらす可能性があるシナリオが存在します。たとえば、病気で出社できないと申告していながらフットボールの試合を見に行っていることや、出張中と言いながら快適なビーチで過ごしていることが、ソーシャルメディアネットワークで顔が認識されてばれる可能性があります。さらに、投稿する写真に写っている人物にタグ付けする際に、それが正しいかどうかを友人や親戚に確認する場合もあり

[82] https://ieeexplore.ieee.org/document/5551046

ます。違法な街頭抗議に参加するというシナリオでは、特定の司法管轄区域では逮捕や法的効果につながる可能性があります。

メディアコンテンツが露呈し続ける限り、そのコンテンツを収益化したり、攻撃シナリオの中で特定の人物を利用したりする様々な方法が存在します。また、新しいテクノロジによって、攻撃者が攻撃する機会がますます増えているのも明らかです。

認証への攻撃

認証ベースの攻撃シナリオでは、主な特徴として顔、虹彩、指紋、および声が使用されます。ローカル認証とリモート認証がありますが、このセクションでは、両方のシナリオのさまざまなユースケースについて説明します。

ローカル認証メカニズムの悪用

ローカル認証メカニズムは、センサとセンサによってアクセスが提供される資産の位置が近くにあることを意味します。言い換えれば、生体情報ベースの認証によって生体認証センサに近接する資産へのアクセスが提供されるシナリオは、ローカルであると見なされます。

公共交通決済や次世代小売業がローカル認証カテゴリに分類されるのはそのためです[83]。これらのケースの多くは（指紋ベースのドアロックと同様に）、センサにパターン情報のデータベースが組み込まれています。このデータベースは、スマートフォンやローカルコンピュータにも配置できます。

ノート PC や携帯電話などの機器のロック解除

携帯電話、タブレット、ノート PC など、最新の多くの機器には、何らかの形で生体認証センサが組み込まれています。生体情報によるこれらの機器のロック解除は、日常生活で最も実用化されているユースケースシナリオであり、この分野での攻撃については広く報道されています。攻撃が行われると、ロック解除の痕跡がローカルログに記録されます。しかし、エンタープライズレベルの生体認証システムに比べると、これらの商用機器では、詳細に調査する機能は限定的です。これは、認証がローカルに行われるためです。

露呈した生体情報を使用したデバイスのロック解除攻撃が行われる理由はさまざまであり、デバイスの所有者の社会的役割に応じて大きく異なります。政治家や経営幹部は国家が支援する攻撃の格好の標的であり、その一方で一般人はさまざまな金銭窃取戦略の犠牲になる可能性があります。

[83] https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain

生体認証ドアロックの開錠

生体認証ロックは、有名人の自宅や権力者の高級アパートで広く使用されています。これらのロックが使用されていると、事前登録されている人は物理的な鍵を使用しなくても出入りできます[84]。すでに露呈している生体情報を使ってそのようなロックを不正に解除することができれば、攻撃対象領域が拡大して、財産に物理的にアクセスされる可能性があります。

このようなアクセスは、恐喝から、風評被害、金銭獲得を目的としたシナリオまで、さまざまな結果につながります。最もわかりやすいのは、特に自宅内部の様子（と財産）を定期的に披露し、さらにセキュリティを回避するために必要な詳細な生体情報をすべて露呈しているインフルエンサーが、強盗や窃盗の被害に遭うケースです。

次世代小売業、公共交通決済、および現金引き出し

次世代小売業サービス[85]や公共交通の生体情報ベースの決済システムは、さまざまな国ですでに稼働しているか、プロトタイプとして使用できます。生体情報ベースの認証に対する攻撃が成功した場合、買い物の代金や公共交通チケットの料金が、なりすましの被害者に請求されることにつながる可能性があります。金銭的な影響が大きくない場合もありますが、その場合は法執行機関の捜査対象になる可能性が低くなるという副作用があります。このカテゴリの攻撃の成功により、サラミスライシング攻撃（不正が発覚しない程度の少量の攻撃や金品の搾取を継続する攻撃）の新しいバリエーションとして分類できる場合もあります[86]。

生体認証機能を搭載した ATM がますます増えています。銀行カードを提示しなくても生体認証機能により現金を引き出せる場合、露呈した生体特徴を使用して認証に成功すれば、銀行口座の所有者に直接金銭的影響を与えることにつながる可能性があります。

リモート認証メカニズムの悪用

リモート認証メカニズムは、遠隔地にある資産にアクセスできるようにします。そのわかりやすい例として、オンラインバンキングを使用した銀行口座へのアクセスや生体認証を必要とするクラウドストレージへのアクセスがあります。

リモート認証メカニズムには、ローカルメカニズムに比べて、認証側からセンサ情報の完全性やセンサが置いてある環境を制御および監視する能力が限定的であるという重要な特徴があります。人物が建物に出入する場合、その場のセンサが制御されている可能性は、攻撃者の制御下にある環境に取り付けられ、リモート資産にアクセスするために使用されるセンサに比べて、はるかに大きくなります。

---

[84] https://www.dailymail.co.uk/femail/article-10831465/Real-Housewives-Dallas-star-Tiffany-Moon-proudly-shows-3-MILLION-closet.html

[85] https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain

[86] https://howtoinfosec.com/2021/06/11/what-is-salami-attack

攻撃者は、たとえば、照明条件を選択すること、指の人工的なコピーを使用すること、およびセンサ出力を偽装することを、それらのデータが認証用バックエンドに送信される前に、すべて実行できます。ただしこのことは、リモート認証シナリオの攻撃対象領域は一般にローカル認証シナリオの場合に比べて広くなることも意味します。

リモート認証の主なユースケースは、アカウントの認証および取引の確認です。生体認証には、2 要素認証（2FA）を回避して、攻撃者が被害者の iCloud アカウントへのアクセスを取得するのに使用できる既知の脆弱性があります[87]。リモート指紋認証に関するさまざまな研究も実行されています[88]。

組み込み機器によるアカウント照会や金融取引の確認

多くの金融アプリまたは金融取引を開始できるアプリは、機器に組み込まれた生体情報収集機能を使用して、アクセスを提供したり、取引を確認したりします。たとえば、多くのモバイル銀行アプリは、標準の 2FA 手順を実行する代わりに、組み込まれている指紋スキャナまたは顔認識機能を使用して取引を確認できます。生体認証の回避に成功すると、なりすましの被害者に直接的に金銭的影響を与えることができます。

もう 1 つのユースケースとして、信頼できるストアまたは信頼できない提供元からでも、ソフトウェアをインストールする、アカウントをホストに追加する、機密ドキュメントを編集するなどのデバイス上での機密性の高い操作の実行を確認することがあります。

将来のデバイス

生体情報を収集して処理する機能を備えた IoT／IIoT デバイスがますます増えることが予想されています。たとえば、仮想現実／拡張現実デバイスに搭載される生体認証機能は増加するでしょう[89]。攻撃者は、そのようなデバイスをだますことによって、メタバースやゲームのさまざまなデジタル資産にアクセスできるようになります。デバイスがハイテク生産工程などで使用されている場合は、スパイ機能すら入手できます。

次世代自動車などの物的資産も、近い将来影響を受ける可能性があります。生体情報ベースのキーレスカーアクセスが近い将来大規模に展開されることが予想されており[90]、生体認証アルゴリズムへの攻撃に成功すると、高価な物的資産に影響が及ぶ可能性があります。

[87] https://www.biometricupdate.com/202008/hackers-may-have-manipulated-apple-biometric-security-glitch-to-access-icloud-accounts

[88] https://arxiv.org/pdf/1805.07116.pdf

[89] https://dl.acm.org/doi/abs/10.1145/3457339.3457983

[90] https://www.cambridge-news.co.uk/news/motors/six-ways-driving-your-car-24291332

読者の皆様に伝えたいこと

近年、社会では個人情報の露呈について多くの疑問が投げかけられています。多くの司法管轄区域がすでに一歩踏み込んで、個人情報処理のルールを明確にする一般データ保護規則（GDPR）[91]などの法律や生体データ処理の一部のユースケースに対する規制ガイドラインを受け入れています[92]。大きな問題は、これらの法律や規制は特定の司法管轄区域に関連付けられているのに対して、コンテンツの露呈はグローバルに発生する点です。グローバルな露呈の副作用として、近い将来、組織や個人が生体データを処理して収益化できるようになります。

このセクションでは、生体パターンの露呈のリスクと影響の抑制に役立つ推奨事項について説明します。また、一般の人々に向けての提案と、生体情報を所有、処理、加工、または使用する特定のグループに向けての提案を示します。

生体認証が他の認証や本人確認の方法と異なる点

人物の顔、指紋、虹彩パターンなどの生体特徴は、パスワードのように簡単に変更することはできません。それらが漏えいした場合、10 年、またはそれ以上の期間にわたる影響を引き起こす可能性があります[93]。

場合によっては、10 代のころに発生した非意図的な生体情報の漏えいが、一生にわたって影響を及ぼす可能性もあります。一方、デバイスの操作方法、キーボードを叩くリズム、デバイスを手に持つ角度などの動的生体情報は、より柔軟です。ただし、デバイスが侵害された場合、それらの痕跡はテレメトリレベルでプロファイリングされ、置き換えられる可能性があります。

人々は、自分の生体特徴は決して自分から離れませんが、その情報が離れてしまうと、露呈した他のデジタル資産と同様、複製されて手に負えない形で拡散される可能性があることを認識する必要があります。同時に、生体情報が露呈したインシデントの影響を緩和するための手段は、パスワードや露呈したクレジットカードデータなどの機密性の高い資産に比べて、はるかに限定的です。

一般の人々への提案

一般の人々に向けて、以下のベストプラクティスを推奨します。

- **生体パターンの露呈を最小限に抑える。**現代生活では、顔のパターンや声紋を露呈しないようにするのは、もちろん非常に難しいことです。しかし、ほとんどのインターネッ

[91] https://gdpr-info.eu

[92] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

[93] https://www.npr.org/2019/01/20/686897486/could-the-10-year-challenge-be-putting-your-data-at-risk?t=1657982303769

トユーザにとって、それ以外の指紋や虹彩パターンなどの生体パターンの管理を最小限に抑えることはできます。

- **一般に公に露呈する、あるいは露呈する可能性が高い、生体要素への依存を最小化する。**リモートバンキング取引を確認するための認証に顔認識を使用することは、露呈することが少ない生体要素を使用する場合に比べてリスクが高くなる可能性があります。
- **露呈するメディアまたは生体特徴が含まれる可能性がある部分のメディアの品質を最小化する。**あるいは、人間に感知できなくとも、コンピュータにとってはまったく異なるものとなるランダムな方法で、このデータを透過的に操作することを検討してください。たとえば、写真の虹彩パターンを変更すると、コンピュータのみが認識可能な差異が生じます。
- **公共メディアに広く登場し、高解像度で記録される人物の場合、意味のある生体データはすべて、すでに露呈しているか、または露呈するリスクが非常に高いと想定する。**このような人物の場合、常に生体情報はすでに侵害されていると想定する必要があり、生体情報はあらゆる認証で 2 要素認証の一部としてのみ使用するべきというリスク戦略を採用することを推奨します。プライバシーの観点では、これらの人物の名前を明かさずに撮影したメディアであっても、今後ますます容易に現実の ID に結び付けられる可能性が高いことを想定する必要もあります。

生体情報を処理する組織に向けた提案

- 信頼できる環境と信頼できない環境では異なるセキュリティプロセスを使用します。信頼できる環境とは、組織または信頼できるパートナーのセンサによって監視および制御されている環境のことです。信頼できない環境とは、生体特徴を投稿した人物によって管理されているセンサまたは環境のことです。
- 重要ではない資産またはタスクの場合のみ、1 要素認証として生体情報を使用します。または、「本人の特徴による認証」だけでなく、「記憶による認証」を使用する MFA の 1 つの要素としてのみ生体情報を使用します。信頼できない環境の場合は特に、このことを考慮する必要があります。
- 生体情報を使用するビジネスプロセスに関わるストレージ、処理、およびライフサイクル全体のセキュリティを確保します。
- 発生する可能性があるデータ侵害の影響を最小化するよう生体パターンを保護します。

ディープフェイクの存在について、特に電話会議に導入される可能性があるリアルタイムでの偽装を中心に、注意を払います。

自分の生体情報を扱う方法

守るべき共通のアドバイスとして、次の 6 つの黄金律を推奨します。

- 露呈するリスクがある主要な生体情報タイプである顔、声、指紋、掌形、および虹彩に

注意すること。

- すべての生体特徴、特に指紋、掌形、および虹彩パターンの露呈を制限すること。
- 露呈するメディアの品質を最小化し、投稿するメディアの中で機密性の高い部分を変更すること。
- 意図的な露呈を目的として何かをオンラインで共有する前に、慎重にメディアを確認すること。
- メディアプラットフォーム上でアクセス権限を正しく制御および管理すること。
- 定期的に自分の画像のメディア検索を実行して、画像が出現しているコンテキストをチェックすること。これには、Google Images[94]や Yandex Images[95]などの逆画像検索が役立ちます。これは、自分の画像の悪用を抑制し、風評被害を最小化できる評判管理手法の 1 つです。たとえば、攻撃者は、人物の本物の画像を悪用することもできるし、その人物のディープフェイクを作成して悪用することもできます。

一般的な提案に加えて、読者の皆様には次のことについても考慮することを推奨します。

- 生体情報を使用する場合、ネットワークセグメンテーションと同様の戦略を使用するという選択肢があります。すなわち、生体情報を使用する可能性を、政府サービスの利用、金融、建物の出入などのセグメントに分割します。生体特徴自体はそれぞれの公開しやすさに従って優先順位を付けます。たとえば、顔と声は簡単に公開できますが、それらに比べれば指紋と虹彩パターンは公開が困難です。認証するアカウントまたはサービスの機密性によっては、露呈しづらい特徴を使用します。
- 本人確認には、公に露呈している可能性がある生体情報を使用します。認証には、公に露呈していない生体情報を使用します。
- 1 要素生体認証には、露呈していない可能性がある生体情報を使用します。他の選択肢がない場合、露呈している可能性がある生体情報を、1 要素としてではなく、MFA の一部として使用します。複数の種類のサービスで指紋が必要な場合、サービスごとに異なる指を使用するか、左手と右手を交互に使用します。
- リモート認証とローカル認証および監視付き認証と監視なし認証で、必須要件と希望要件を分離します。出入国管理を通過する場合、画像を使用して認証できます。しかし、自宅からリモートネットワークへのログインを認証する場合、シナリオはまったく異なります。
- 生体情報を新しい種類のサービスや技術に露呈する場合、十分に注意してください。新しく登場したテクノロジは、多くの場合、規制がまったく存在しないか、少ないことを意味します。その場合、露呈したデータが悪用される可能性が高くなります。
- メディアコンテンツを作成する場合、特にプロ用機材を使用する場合、露呈を最小化するために機材そのものの使用を工夫します。これはまさに政治家、CEO、および有名人のケース

[94] https://images.google.com

[95] https://yandex.com/images

に、特にライブストリーミングのシナリオで、当てはまります。たとえば、分散した複数の光源を使用すると、虹彩に多重反射が生じるので、露呈する領域を最小化できます。光の点を 1 つ使用すると、それが瞳孔の真ん中で反射して、露呈したメディアから虹彩の収集に成功する可能性が高くなります。

図 20：公開されている YouTube 動画の複数の光源（左）と単一光源（右）の反射の比較[96]
画像クレジット：Jazmin Castro/YouTube

[96] https://www.youtube.com/watch?v=7CjGM2grg_0&ab_channel=JazminCastro

まとめ

生体データは、絶対に期限切れにならないパスワードのように扱う必要があります。現時点では犯罪者はこの情報を使用して確実に大規模な攻撃を行うことはできませんが、だからといってずっとそれが続くわけではありません。

最近のいくつかのケースでは、攻撃者が漏えいしたデータを使用する攻撃を計画して実行するために、被害者の所有する電話やノート PC などの物理デバイスにアクセスする必要があることが確認されています。これは支配力の強い侵害シナリオの中でも憂慮すべきシナリオですが、これも社会で生体情報が使用されることが増えるにつれて変化するでしょう。

長年にわたって、人々は機密性の高い自分の生体情報データを、意図的および非意図的にインターネットに露呈してきました。しかし、非意図的な露呈は、シェアした人物が露呈していることに気付いていないので、意図的な露呈よりダメージが大きくなる可能性があります。

ユーザである私たちは、露呈したデータを管理できなくなっています。また、露呈したデータの将来的な用途や私たちが日常的に使用するプラットフォームのリスクは、一般ユーザには十分に理解されていません。実際、ソーシャルメディアネットワークのデータは、すでに政府やスタートアップ企業によって、生体情報を抽出して監視カメラ用の識別モデルを構築するために使用されています[97]。

それと同じデータが、私たちの生活の中で最も機密性の高い部分で現在使用されており、今後も使用されるでしょう。たとえば、銀行口座の使用、公共交通機関や次世代店舗でのキャッシュレス決済の使用、国境の通過、キーレスドライビング、または警察官であれば犯罪の捜査に使用します。生体データの特質として、各個人が、パスワードと違って変更できない限られた数の生体特徴（指紋、顔、声、虹彩、網膜、掌形など）を持っています。

生体データは変更できないという事実は、将来そのようなデータの宝庫の存在が犯罪者にとってますます有益であることを意味します。その将来が 5 年後であろうが 20 年後であろうが、データを現在すでに入手可能なのです。明日の世界で自分を守るために今日予防策を講じることを、将来の自分に対する義務と捉えるべきでしょう。

それとともに、データの可用性、データマイニングテクノロジの発展、人工知能、および PII によるデータ侵害の存在により、露呈した生体データを使用できる攻撃対象領域は大幅に拡大しています。これは、将来、地球上のほぼすべての人に影響を及ぼす可能性があります。

本書では、ソーシャルメディアプラットフォームやメッセージングプラットフォームですでに大規模に露呈している生体特徴から生じる重要なリスクを取り上げました。攻撃者は、収集したデータを使用して、機密性の高い金融サービスや行政サービスの本人確認と認証を回

[97] https://ntechlab.com/en_au/solution/public-safety

避できます。もちろん、生体認証が必要な制限区域への出入、デジタル ID の窃盗、評判システムと社会信用システムの侵害、ディープフェイクの作成、および法執行機関に警告を発することも可能です。

露呈した生体データの問題は、人類が対処する必要がある難問です。トレンドマイクロは、次の対策を推奨します。

- 高品質なメディアにおける非意図的な露呈を最小化する。
- 機密性の高い区域への出入には、特にリモート認証の場合は、露呈することが少ない生体パターンの使用を優先する。
- 静的および動的な生体情報と他の手法を組み合わせて認証に使用する。
- 現在と将来の両方の活動で、現在および過去に露呈している生体データを使用されることに対処するという重要な方針変更を行い、この問題に大規模に取り組む。

トレンドマイクロは、生体情報ベースのテクノロジを使用、提供する組織または一般の方が、読者の皆様の生体情報を露呈した際にもたらされる新たなセキュリティリスクを最小限に抑える為に、本書のような注意喚起と紹介した提案内容が役立つことを期待しています。さまざまなサービスで世界中の人々の本人確認と認証を行うという難問を解決する為の手法開発は、これからも進化と前進を続けるでしょう。本書で提起した懸念の一部が、より詳細な議論につながり、社会にとってより良い全体的な解決策を促すために役立つことを期待しています。

付録

現実世界のデバイスに対する露呈データを用いた侵害テスト

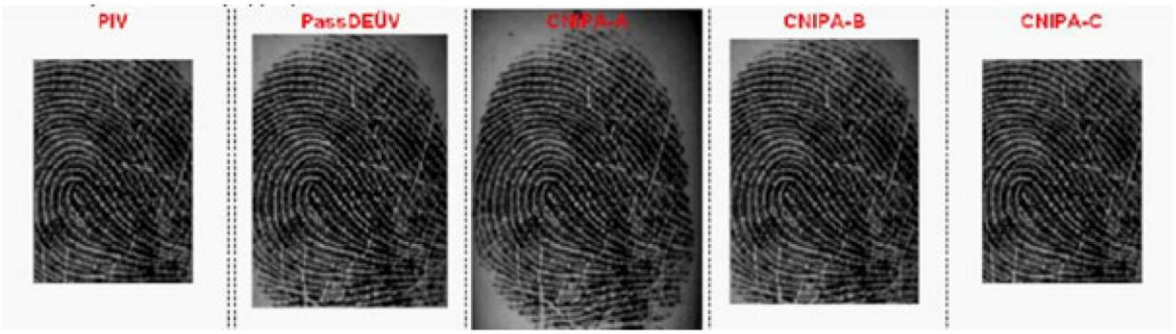
トレンドマイクロは、認証に広く使用されている指紋、顔、および虹彩の 3 種類の特徴に関連する侵害シナリオを調査しました。すべてのケースにおいて、独自の調査または外部の信頼できるソースのどちらかで、評価しようとしている脅威やリスクが存在することが確認されました。

この調査では、非意図的に漏えいした指紋を使用してソーシャルメディアに掲載されている写真から人物の本人確認を実行できるのか? 高度な技術を持たない攻撃者でも顔認識機能付きのカメラをだますことができるのか? ハードウェア虹彩センサのアルゴリズムを他の被写体でだますことはできるのか? ソーシャルメディアで露呈しているメディアコンテンツの解像度は虹彩センサ等で人物を登録または認証するのに十分な精度をもっているだろうか? といった質問への回答を試みました。

このセクションでは、生体認証システムを処理、攻撃、およびだますこと、または露呈している指紋、顔、および虹彩を用いて意思決定することを可能にするテクノロジと機能に焦点を当てます。

指紋

指紋は通常、8 ビット／ピクセルのグレースケール形式で取得され、推奨解像度は 500 ピクセル／インチ（197 ピクセル／cm）以上です[98]。取得領域は、ほとんどの標準で幅 12.8～25.4 mm、高さ 16.5～24.5 mm の範囲で設定できます。これは、指紋の画像は、252 × 325 ピクセル以上であれば、特定の人物の本人確認に十分であることを意味します。



[98] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf

Table 1. A comparison of PIV, PassDEÜV and CNIPA-A/B/C requirements for the main quality parameters.

Parameter	Requirement				
	PIV IQS [4] [9]	PassDEÜV IQS [13]	CNIPA		
			IQS A	IQS B	IQS C
Acquisition area	w ≥ 12.8mm h ≥ 16.5mm	w ≥ 16.0mm h ≥ 20.0mm	w ≥ 25.4mm h ≥ 25.4mm	w ≥ 15.0mm h ≥ 20.0mm	w ≥ 12.8mm h ≥ 16.5mm
Native resolution	$R_N \geq 500$ppi				
Output resolution	$R_N \pm 2\%$	$R_N \pm 1\%$	$R_N \pm 1\%$	$R_N \pm 1.5\%$	$R_N \pm 2\%$
Gray-level quantization	256 gray-levels (8 bpp)				
Geometric accuracy	In 99% of the tests: $D_{AC} \leq \max\{0.0013'', 0.018 \cdot X\}$ $D_{AL} \leq 0.027''$	In 99% of the tests: $D_{AC} \leq \max\{0.0007'', 0.01 \cdot X\}$ $D_{AL} \leq 0.016''$	In all the tests: $D_{Ref} \leq 1.5\%$	In all the tests: $D_{Ref} \leq 2.0\%$	In all the tests: $D_{Ref} \leq 2.5\%$
Input/output linearity	No requirements	$D_{Lin} \leq 7.65$	No requirements		
Spatial frequency response	$MTF_{min}(f) \leq MTF(f) \leq 1.12$ see [1] for PIV $MTF_{min}(f)$	$MTF_{min}(f) \leq MTF(f) \leq 1.05$ see [1] $MTF_{min}(f)$ values	For each region: $TSI \geq 0.20$	For each region: $TSI \geq 0.15$	For each region: $TSI \geq 0.12$
Gray level uniformity	In 99% of the cases: $D_{BC}^{dark} \leq 1.5$; $D_{BC}^{light} \leq 3$ For 99% of the pixels: $D_{PP}^{dark} \leq 8$; $D_{PP}^{light} \leq 22$ For every two small areas: $D_{SA}^{dark} \leq 3$; $D_{SA}^{light} \leq 12$	In 99% of the cases: $D_{BC}^{dark} \leq 1$; $D_{BC}^{light} \leq 2$ For 99.9% of the pixels: $D_{PP}^{dark} \leq 8$; $D_{PP}^{light} \leq 22$ For every two small areas: $D_{SA}^{dark} \leq 3$; $D_{SA}^{light} \leq 12$	No requirements		
Signal-to-noise[1]	SNR ≥ 70.6	SNR ≥ 125	SNR≥70.6	SNR≥49.4	SNR ≥30.9
Fingerprint gray range	For 80% of the images: DR ≥ 150	DR ≥ 200 for 80% images; DR ≥ 128 for 99% images	For 10% of the images: DR ≥ 150	For 10% of the images: DR ≥ 140	For 10% of the images: DR ≥ 130

図 21：パラメータごとの指紋情報の収集品質要件[99]
画像クレジット：A. Alessandroni et al/CiteSeerX

指紋ベースの生体認証が議論されるようになってから聞かれるようになったのが「指紋センサをだますことができるのか?」という質問です。

答えは単純で、「はい」です。指紋センサを突破する方法とそのようなセンサのセキュリティを強化する方法を示す数十件のアプローチを学術論文で見つけることができます。中には、センサをだますために作成した偽造指の画像を掲載している論文すら存在します[100]。

図 22：20 人の被験者の人差し指、中指、および親指をモデル化した、多数の高精度な偽造指[101]
画像クレジット：Aditya Singh Rathore et al/Network and Distributed Systems Security (NDSS)

[99] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.566.4224&rep=rep1&type=pdf
[100] https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf
[101] https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf

当社が定期的にレビューしている論文には、さまざまなレベルのデバイスに対する指を用いたなりすまし攻撃の成功率統計が掲載されていました。スマートフォンやノート PC でよく使用されている部分的指紋センサの場合、成功率がほぼ 90%に達する場合があります[102]。全体指紋を使用する専用デバイスの場合、成功率は下がりますが、それでもなりすまし攻撃を重大な問題として検討するには十分な成功率の高さです。

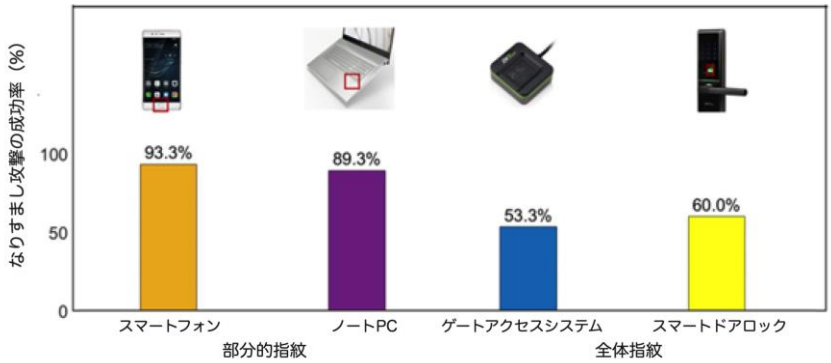


図 23：高精度な偽造指によるなりすまし攻撃の成功率

指紋ベースの認証において、センサはパズルの 1 つのピースに過ぎないことに注意することが重要です。デバイスに保存されている指紋データも攻撃される可能性があります。悪意のあるプロセスが指紋センサへのアクセスを取得し、被害者の指紋を収集する場合もあります。これらの攻撃については、セキュリティカンファレンスですでに説明されており[103]、生体情報ベースの本人確認・認証センサをだますことができる方法が確認されています。大規模に展開または分散されているシステムでは、攻撃対象領域がさらに拡大します。

本書では、ソーシャルメディアで露呈している生体特徴のリスクを取り上げます。このコンテキストで重要なのは、写真を使用して人物を再現、登録、または認証できるかどうかを知ることです。この場合も答えは「はい」であり、そのようなシナリオが複数確認されています。初めて確認されたのは 2019 年であり、「darkshark9」と呼ばれる研究者が自分の指の 3D モデルを印刷して、Samsung Galaxy S10 のロックを解除できました。まず、ワイングラスに付けた指紋の写真を使用して、その指紋から Adobe Photoshop でアルファマスク（選択した領域以外をマスクし、特定領域を抽出する技術）を作成しました。次に、Autodesk 3ds Max ソフトウェアで高精度の 3D モデルを作成しました。この 3D モデルを、AnyCubic Photon LCD resin printer を使用して、指紋のすべての隆線を正しくレンダリングできる品質で印刷しました。最後に、印刷した指モデルを使用して、スマートフォンのロック解除に成功することができました[104]。

[102] https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf

[103] https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf

[104] https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/?sh=1fe040755d42

2020 年には、Cisco Talos の複数の研究者がさまざまなデバイスの指紋スキャナの突破をテストして、平均 80%の成功率を達成しました。また、3D プリンタを使用して偽造指を生成し、2,000 米ドル以下の予算で攻撃を実行しました。この研究では 3 つの指紋収集シナリオをテストしました。1 番目のシナリオでは標的に該当する指紋の型直接収集し、2 番目のシナリオでは国境検問所にあるようなスキャナから収集したセンサデータを使用し、3 番目のシナリオでは標的が手に持っていたボトルなどの物体から指紋を浮き上がらせました。注目すべきは、Apple の MacBook Pro 2018 Touch ID も、研究者がだますことに成功したデバイスの 1 つだということです[105]。

上記の 2 つの例は、指紋センサを回避するには、通常は指紋の写真があれば十分であることを裏付けています。本書のコンテキストで残っている唯一の疑問は、本書の範囲の制約がある中で、指紋ベースの本人確認と認証をだますことができるかどうかということです。もっと正確に言うと、「公に露呈している指紋の画像を使用して、人物を本人確認することまたは指紋ベースのセキュリティメカニズムを回避することができるのか?」という質問になります。どちらの質問も、答えは「はい」です。

2 つのケースで、警察が露呈しているメディアコンテンツを使用して犯罪者を追跡していることがわかりました。1 番目のケースでは、リバプールの麻薬の売人がオンラインチャットでスティルトンチーズの写真を共有した後、その写真から指紋と掌の情報が露呈し、それによって本人確認が行われました[106]。2 番目のケースでは、指紋のデジタル画像が、フィンランドの詐欺事件の解決に役立ちました[107, 108]。

2014 年のカオスコミュニケーション会議で、生体情報ハッカー兼プログラマである Jan Krissler 氏が、ソーシャルメディアで露呈している写真からの指紋パターンの再現に関連する興味深い研究について発表しました。Krissler 氏は、当時のドイツ国防相である Ursula von der Leyen 氏のプレスリリースの写真などのさまざまな高解像度写真を使用して、Leyen 氏の指紋をリバースエンジニアリングしました[109]。今日の最新のモバイルデバイスはますます高度化しているので、オンライン上の写真の品質も、2014 年ごろから大幅に向上していることは注目に値します。

まとめると、これらのケースは次のことを意味しています。

- 攻撃者が、スマートフォンやノート PC の組み込み指紋センサなど、さまざまな指紋センサをだますことができる。

---

[105] https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/?sh=1fe040755d42

[106] https://www.bbc.com/news/uk-england-merseyside-57226165.amp

[107] ttps://twitter.com/mikko/status/1535209158995329024

[108] https://poliisi.fi/-/petosrikos-selvisi-tekniikan-avulla

[109] https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

- 写真や動画を使用して、認証に必要な指紋パターンを再現できる。
- 公共メディアのコンテンツの品質は、メディアで露呈している指紋から情報を取得し、不正活動に利用するのに十分な精度である。

顔認識

顔認識はさまざまな手法で行われます。最も単純な方法としては、Web カメラ、さまざまな IoT デバイスの組み込みカメラ、スマートフォンなど一般的なカメラで輪郭を認識します。より高度な手法では、入手した画像の照明の影響が少ない近赤外域を使用します[110]。

セキュリティを強化するために、数千個の目に見えないドットの投影により顔の特徴の詳細情報を収集する技術や、最近の研究で人間より優れているとされている機械によるライブネス検出などの機能が追加されています[111]。

顔認識に必要な画質に関して、ISO/IEC 19794-5（生体データ交換形式）など、さまざまな標準および最小要件が存在します。また、米国標準技術研究所（NIST）の Ongoing Face Recognition Vendor Test（FRVT）[112]の照合要件である露呈した顔の画像も、本書の範囲に含まれると見なすことができます。次に示すのは、NIST の論文に掲載されている画像の例であり、640 × 480 ピクセルの縦方向の画像は顔認識に十分であると述べています。これは、この解像度品質が、広く使用されている多数のカメラやデバイスで長年にわたって使用されてきたことを意味します。

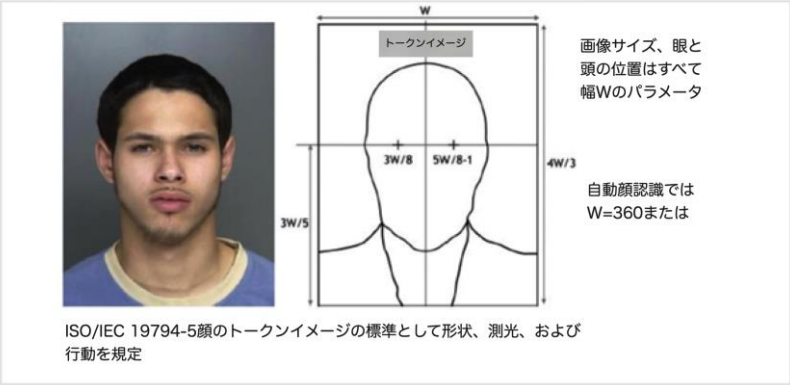


図 24：顔認識用画像のパラメータ[113]

画像クレジット：Patrick Grother et al/National Institute of Standards and Technology (NIST)

エッジデバイスのセキュリティを調査した最近のプロジェクトでは、顔認識デバイスに対するさまざまな攻撃が成功することがトレンドマイクロの研究者により実証されています。そ

[110] https://www.sciencedirect.com/science/article/abs/pii/S1574013716300673?via%3Dihub

[111] https://www.idrnd.ai/wp-content/uploads/2022/01/ResearchBrief-HumanVsMachine-JAN2422.pdf

[112] https://pages.nist.gov/frvt/reports/quality/frvt_quality_report.pdf

[113] https://pages.nist.gov/frvt/reports/quality/frvt_quality_report.pdf

のシナリオには、モバイルデバイスで表示された静止写真を使用した顔認識の回避など、さまざまな攻撃チェーンの実証が含まれています[114]。

より高度なセンサには、なりすまし攻撃を防ぐことに役立つ重要な機能としてライブネス検出が搭載されている場合があります。ライブネス検出の回避に成功する攻撃シナリオも、セキュリティカンファレンスで実証されています[115]。顔 ID を検出するアテンション機構を回避するために、次の試作品が使用されました。

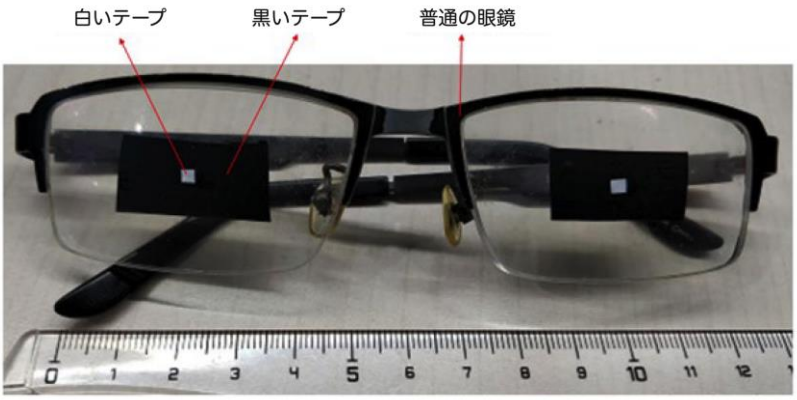


図 25：BlackHat USA 2019 で発表された顔 ID を検出するアテンション機構を回避するために使用された眼鏡の試作品[116]
画像クレジット：Yu Chen, Bin Ma, HC Ma/BlackHat

明らかに、人間の顔は、攻撃者が悪用できる、最も公に露呈している生体特徴の 1 つです。このことは数十本の研究論文ですでに確認されているので、ここでは公共メディアでの露呈という観点で調査されることが少ない生体特徴、すなわち虹彩認識について、さらに深く掘り下げることにしました。

虹彩認識

虹彩認識は、自動化された出入国管理システム、データセンターのサーバルームへの入退室、政府施設への出入など、より機密性の高い区域でよく使用されています。メディアコンテンツでの虹彩パターンの漏えいは、音声記録での声紋の漏えいまたは肖像写真や動画での顔パターンの漏えいほどはっきりとは発生していません。トレンドマイクロの以前の研究で顔認識システムへの攻撃が成功することが確認されているので、ここでは虹彩パターンの考えられる悪用について、さらに深く分析および調査することにしました。

研究では次の疑問を提示しました。

[114] https://documents.trendmicro.com/assets/white_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf
[115] https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf
[116] https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf

- 露呈しているソーシャルメディアコンテンツの品質は、眼のパターン情報の登録または認識に十分なのか?
- 露呈している眼のパターンまたは別の物体の写真が、ハードウェア虹彩センサで眼として検出される可能性はあるのか?
- 画像からパターン情報を登録し、画像を使用して認証することは可能なのか?
- 特定の状況下でのある人物のパターン情報が、別の人物のものとして認識される可能性はあるのか?
- ソーシャルメディア画像からパターン情報を登録し、実物の眼として使用して認証することは可能なのか?
- 実物の眼を登録し、ソーシャルメディアの画像を使用して認証することは可能なのか?

これらの質問に答えるために、漏えいしている画像の解像度が使用するのに十分であることを確認する初期分析を実施しました。次に、ハードウェア虹彩センサ（IriShield-USB MK 2120U）を購入し、一連の実験を実施しました。このセクションでは、実施した研究に対する洞察について説明します。

検出と認識のベースラインは何か?

センサによる虹彩の処理方法およびベースラインが何かを理解するために、1 人の研究者の虹彩を複数回登録しました。次に、登録された同じ虹彩の認識を実施した後、未登録の虹彩の認識を実施しました。

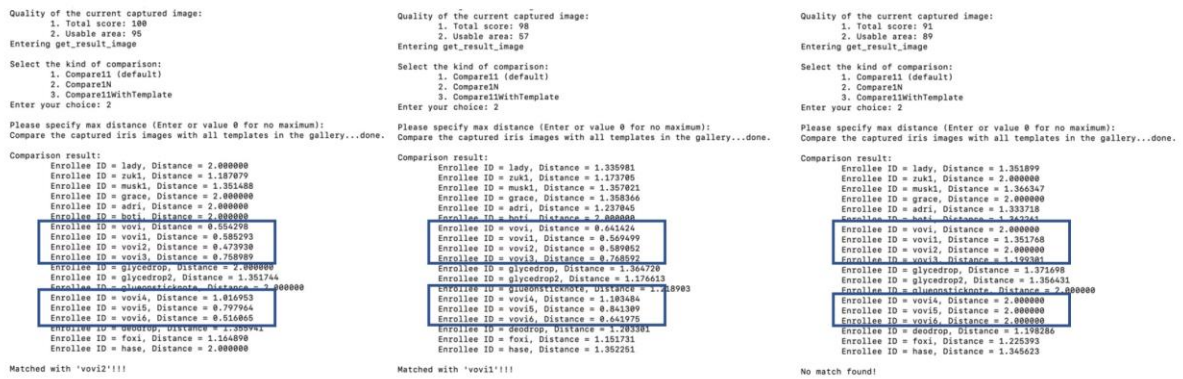


図 26：パターン認識のベースライン：完全な状態で登録された虹彩（左）、目を部分的に閉じているわずかに劣化した状態で登録された虹彩（中）、完全な状態で未登録の虹彩（右）

スクリーンショットでは、ほぼ理想的な状態（使用可能領域 95、総得点 100）では、一致する必要がある既知のパターンの場合の距離はおよそ 0.5～0.8、登録されている他のパターンの場合はおよそ 1.2～2.0 です。劣化した状態（使用可能領域 57、総得点 98）では、一致する必要がある既知のパターンの場合の距離はおよそ 0.6～0.9、他のパターンの場合はおよそ 1.2～2.0 です。未登録パターンを認識しようとした場合はおよそ 1.2～2.0 であり、同じ比率が維持されています。

この観察結果から、この実験では、最大距離が 0.8～1.2 であれば、成功として認められます。0.8 未満のより厳しい距離にすると、攻撃の成功率を大幅に増やすことができます。

露呈しているメディアコンテンツの品質は、眼のパターンの登録または認識に十分なのか?

政府や企業の公式 Web サイト、ジャーナル、およびニュースサイトに掲載されているさまざまなメガピクセル解像度の多数の肖像写真は、虹彩処理に適している可能性があります。

ISO/IEC 19794-6:2011 – 情報技術 – 生体認証データ交換フォーマット – パート 6：虹彩画像データ[117]によれば、VGA 解像度の 640 × 480 ピクセルは眼に適しており、JPEG 2000 形式と PNG 形式は圧縮に適しています。NIST の代替標準[118]では、虹彩の場合は解像度が約 160 ピクセル（またはピクセルスケールが 12.3～15.7 ピクセル／mm）であれば、虹彩認識には十分であることを示唆しています。このスケールは、一般公開されている多数の商用／プロ用肖像写真に広く見られます。

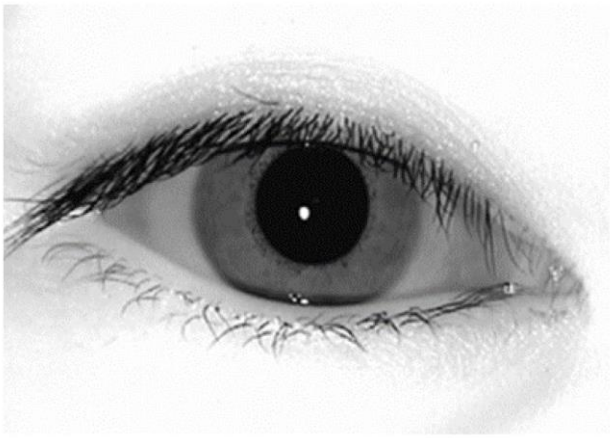


図 27：ISO/IEC 19794-6:2011 で提供されている、虹彩認識に適した眼の画像の例

この研究では、ハードウェア虹彩センサによるブラックボックス分析を実施しました。ブラックボックス分析とは、デバイスのケースを開けずにその電子機器を分析し、ベンダが提供する標準のファームウェアとツールを使用して実験を実施したことを意味します。

その結果、虹彩パターンを登録または認識できるようになる前に、さまざまな予備段階が必要であることがわかりました。デバイスは、稼働を開始すると、近赤外域で一連のフレームを収集して分析します。初期分析の目的は、眼の情報がデバイスに投影されているという事実を認識することです。次の段階では、虹彩を見分けて、投影されたパターン情報の品質を分析します。テストしたデバイスでは、この品質に使用可能領域とトータルスコアの 2 つの基準がありました。実験で得られた結果に基づくと、どちらも 0～100 の範囲で測定されていると思われます。

[117] https://www.iso.org/standard/50868.html

[118] https://www.nist.gov/system/files/documents/2021/06/07/idqt_testplan_draft_v7_6.pdf

これらの基準がどちらも事前定義されている閾値を超えていれば、アルゴリズムの次の段階が実行されます。この段階では、適切な品質のパターン情報を、システムに登録するか、またはこれまでに保存されたパターンと 1 対 1 または 1 対多で比較するか、どちらかを実行できます。露呈しているメディアコンテンツを使用してこの段階に到達し、通過することは、研究段階の重要な部分でした。

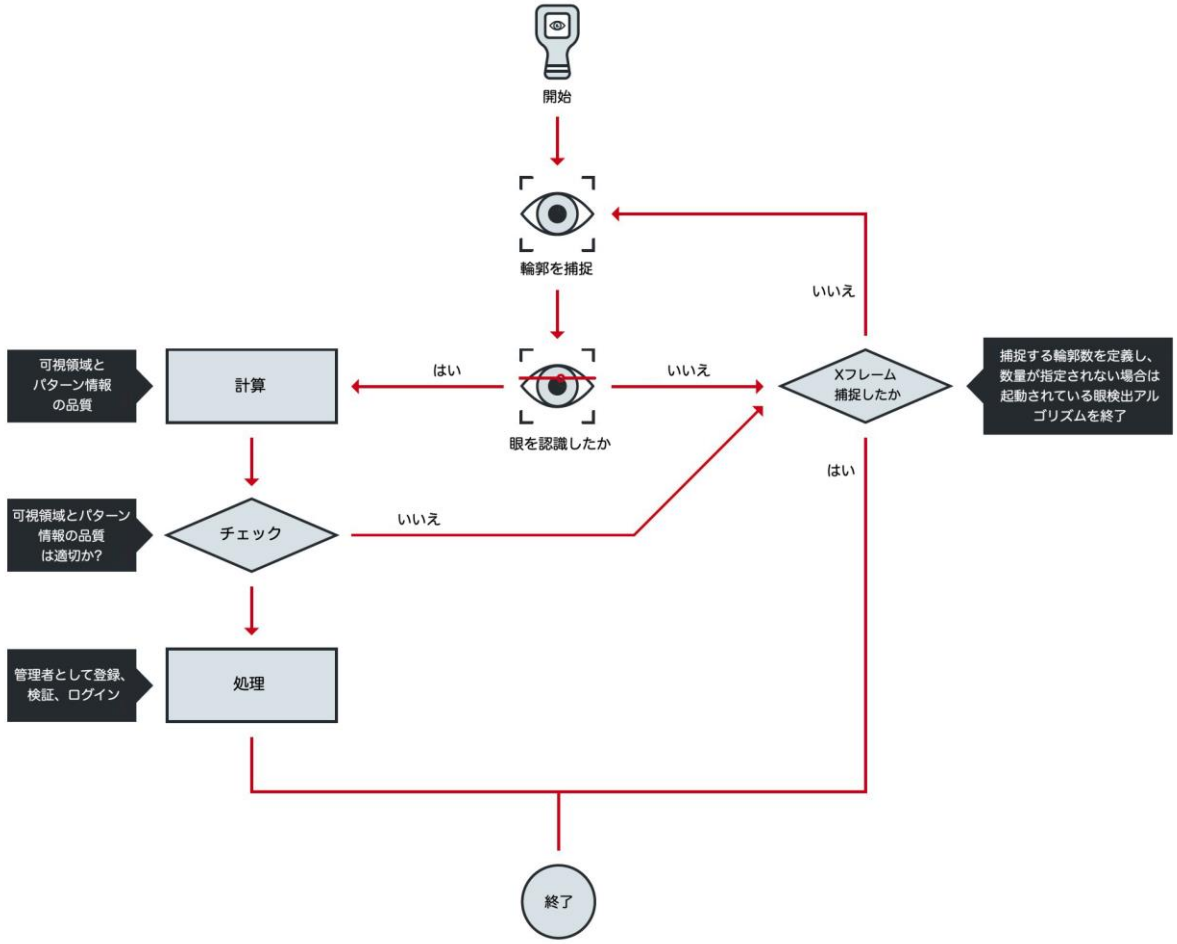


図 28：画像処理ロジック図

虹彩パターンを収集して処理するために、普通のカメラを使用するのではなく、意図的にハードウェア虹彩センサを選択したので、この段階に到達する道のりは決して単純ではありませんでした。このセンサには、攻撃対象領域を最小化するためのさまざまなセキュリティ対策が組み込まれています。

眼を撮影できる焦点距離は限られており、そのため、デバイスに投影されれるパターン情報のサイズも物理的サイズが制限されます。このデバイスには、投影されるパターン情報のサイズを操作するために外部レンズを使用するのを制限するセキュリティ対策も組み込まれています。

実験は、さまざまなスマートフォン外部レンズを虹彩センサに接続して実施しました。その結果、収集した画像の品質が大幅に低下して、眼認識をほとんど実行できませんでした。カ

メラがスマートフォンに組み込まれて虹彩の収集と処理に使用される場合に比べて、これらのセキュリティ対策は攻撃対象領域を大幅に制限していると考えられます。

たとえば、遠く離れた位置にある普通の眼よりはるかに大きい眼の画像をセンサに投影ことはできませんでした。これは、通常のレンズであれば可能であると考えられます。また、虹彩スキャナが近赤外フィルタと内蔵光源を使用しているため、パターン情報をセンサに投影ために画像を収集できるソースが大幅に制限されます。

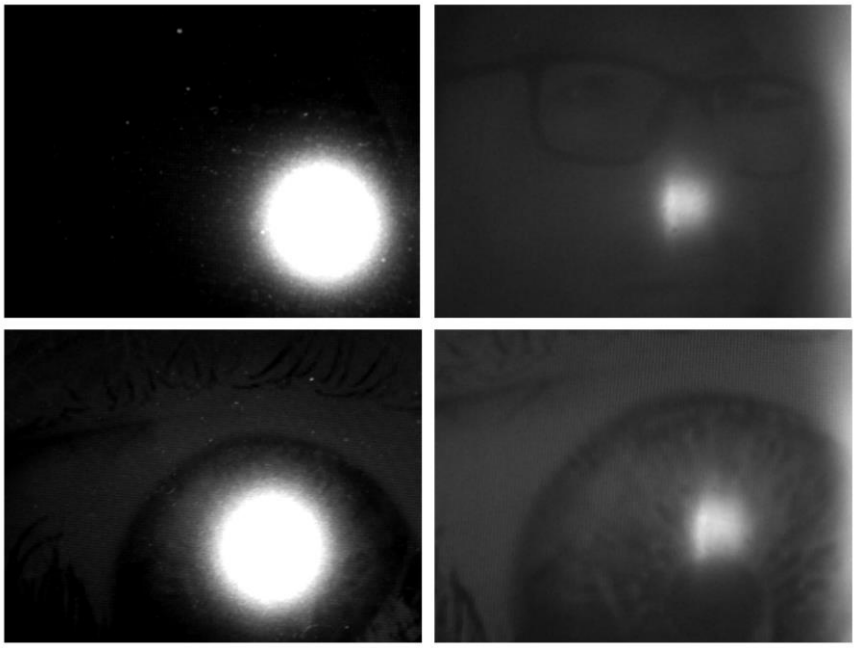


図 29：（上段）Apple MacBook Pro のディスプレイからの画像収集例：標準の収集（左）と光源を隠した収集（右）、（下段）Samsung モニタに表示される眼：標準の収集（左）と光源を隠した収集（右）

ハードウェア虹彩センサのセキュリティ対策により、収集した最初の画像の品質水準は、期待していたものや必要とされるものからかけ離れていました。その後も実験を繰り返して、毎回少しずつ結果を改善していきました。最初の実験の後に明らかになったのは、センサは、眼がセンサに正しく投影されていることを検出するまで、虹彩認識の動作を何も実行しないということでした。

さらに重要なことは、カメラがランダムな物体ではなく人間の眼を認識する方法を理解することは、研究をさらに進めるための鍵となるステップであるということでした。

露呈している眼のパターンまたは別の物体の写真が、ハードウェア虹彩センサで眼として検出される可能性はあるのか?

何度も実験を繰り返した後、眼検出ルーチンを起動するさまざまな画像、形状、および物体を工夫しました。

テストした虹彩センサは、眼を検出すると、青い光を点滅させます。この段階で、使用可能領域やトータルスコアなどのパラメータが収集されます。虹彩パターン認識の実験を続ける

には、この段階をうまく回避することが重要でした。まず、実物の眼を使用して実験を開始しました。その結果、デバイスはほとんど瞬時に眼を検出したことを示しました。次に、ソーシャルメディアで露呈した眼の画像、さまざまな種類の画面に表示された眼、およびさまざまな種類の紙に印刷された眼のテストに移りました。

露呈したメディアについて、当初はあまり成功しませんでした。数日間にわたって何度か眼を認識することに成功しましたが、それには画像の周囲でカメラを動かして、さまざまな角度、距離、および位置から画像を取得するという作業を何度も繰り返す必要がありました。成功した回数は多くありませんでしたが、大きく一歩前進することができました。また、研究をさらに進めるには、眼の検出を回避することが非常に重要であることもわかりました。

眼検出アルゴリズムの仕組みを理解するために、カメラの内蔵光源を使用する場合とそれを隠す場合の両方について、さまざまな照明条件下で一連の実験を実施しました。実物の眼による実験では、内蔵光源を使用する場合の眼の検出が非常に優れていました。ここから眼検出アルゴリズムにおける光反射の役割の重要性に関する仮説を立てました。

眼の検出に成功したときにカメラが取得した画像を比較したところ、瞳孔の中央に位置する明るい白のドットがそれらの画像の重要な特徴の 1 つであることがわかりました。このことを知って瞳孔の中央に複数の半径の白い円を追加するように実験パターンを変更したところ、眼検出率が大幅に向上することがわかりました。

図 30：露呈しているメディアコンテンツから作成したパターン情報の例

実験では、ソーシャルメディアで露呈している画像をさまざまなサイズに拡大縮小して、虹彩センサをだますのに最適なサイズを調べました。この変更により、眼検出率は大幅に向上しましたが、眼検出アルゴリズムの限界を探るためにさまざまな追加実験を実施することにしました。

次の実験では、Microsoft Word で埋め込み図形を使用して眼の完全人工画像を作成し、眼認識アルゴリズムをだますことができるかどうかを調べました。予想と異なり、多くの（すべてではありませんが）ケースでだますことに成功しました。成功するかどうかは、「人工虹彩」の周囲のテクスチャおよび画像のサイズによって決まっていました。

さまざまなサイズで描画した眼の画像を使用して、眼回避アルゴリズムをテストしました。これは、画像を眼として認識するためであり、この眼の画像を以前保存したパターンと一致させるためではないことに注意する必要があります。

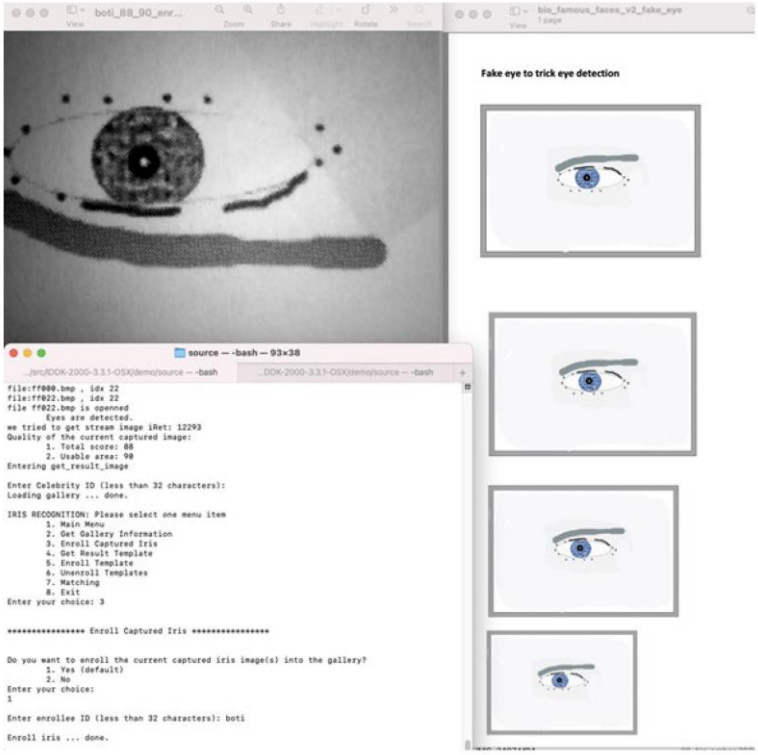


図 31：Microsoft Word で埋め込み図形を使用して作成し、登録で受け入れ可能な品質で認識することに成功した、人工虹彩の「進化版」

これらの結果に基づいて、最大限に単純化した「眼」の中でどれが眼検出ルーチンを起動するのかを調べる追加実験を実施しました。結果は、ほとんどの場合、3 つの単純な円が埋め込まれ、そのうち 1 つにテクスチャと 1 本の線だけが追加されている画像であれば、眼検出ルーチンを起動するのに十分でした。この実験結果を図 32 に示します。

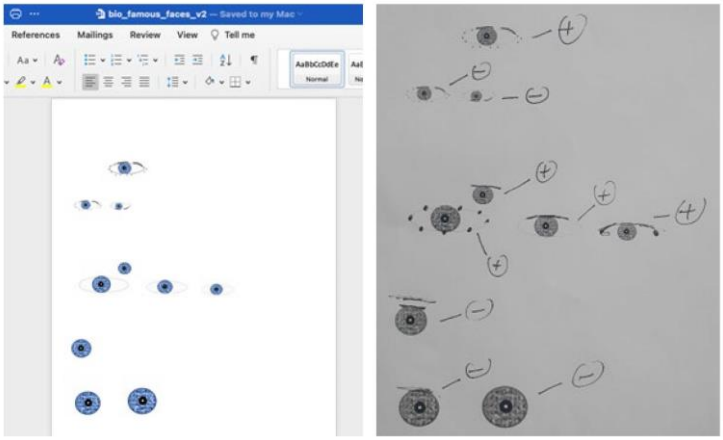


図 32：Microsoft Word で埋め込み図形を使用して作成した最も単純なバージョンの人工虹彩および眼検出の成功／失敗。「+」記号はカメラが画像を眼として認識したことを意味する。

次の実験は、眼に関係ない画像や物体が、虹彩センサによって眼検出を起動できるかどうかを理解するために実施しました。この実験で、眼検出ルーチンを起動するさまざまな種類の物体が見つかりました。実験したのは、さまざまな種類の液体、ぬいぐるみ、および写真の上に透明な接着剤を一滴垂らしたものです。どの種類の物体も、少なくとも 1 回は成功しました。

図 33 に示すぬいぐるみの眼（左）とトレンドマイクロブランドのマウスパッドに液体を一滴垂らしたもの（中）は、眼検出が起動されました。右の図は、眼検出が起動して虹彩センサで取得した画像です。

図 33：ぬいぐるみの眼とトレンドマイクロブランドのマウスパッドに液体を一滴垂らしたものには眼検出ルーチンが起動された

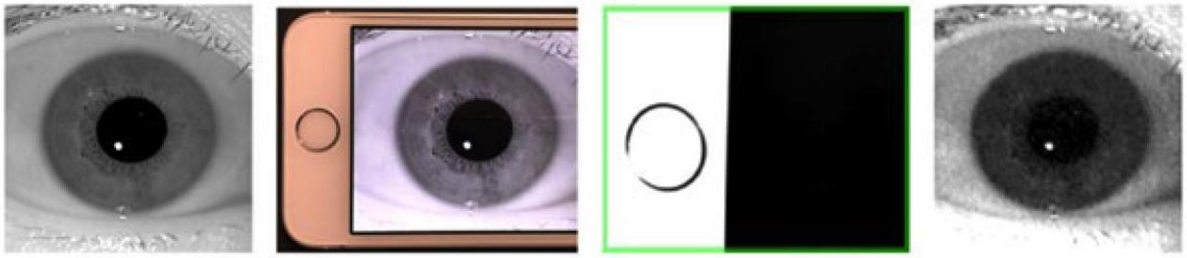
これまでの実験により、カメラの眼検出段階を起動する方法についての理解が大きく進みました。次に行ったのは、パターン認識を対象とした実験です。さらに重要なのは、今回の研究のこの段階で、数百フレームを処理する時間を待つ必要がないことがわかったことです。画像処理の後は、パターンが適切な品質であれば、ほとんど瞬時に眼検出ルーチンを起動できました。

ある画像の眼のパターンを登録し、別の画像を使用して認証することは可能なのか?

答えは「はい」です。インターネットで露呈している肖像写真から収集した虹彩を登録および認識することにも成功しました。

テストに使用した虹彩センサは近赤外光で動作しますが、アクティブディスプレイを搭載するデバイスの画面から取得した画像の品質は大幅に低下します。一方、電子書籍端末の Kindle のようにパッシブディスプレイを使用して、近赤外光でも見える虹彩の画像を表示することもできます。図 34 に、さまざまなメディアで表示した虹彩および iPad カメラと AD 100 虹彩センサで収集した虹彩を比較する画像を示します。これは、arXiv アーカイブ[119]の画像です。

[119] https://arxiv.org/pdf/1804.00194.pdf



(a) 本物の虹彩画像、ノートルダムファイルID：04202d1496。

(b) iPhoneで表示した(a)の虹彩画像をiPadで撮影。

(c) iPhoneで表示した(a)の虹彩画像をAD100虹彩センサで表示。

(d) 電子書籍端末Kindleで表示した(a)の虹彩画像をAD100虹彩センサで撮影。

図 34：さまざまなメディアで表示した虹彩とさまざまなデバイスで収集した虹彩の比較

実験では、インターネットから収集した虹彩の画像を印刷しました。眼検出率を向上させるために、画像にいくつかの細かい修正を加えました。実験では、公開記事や企業の公式 Web サイトからさまざまな肖像写真を選択しました。

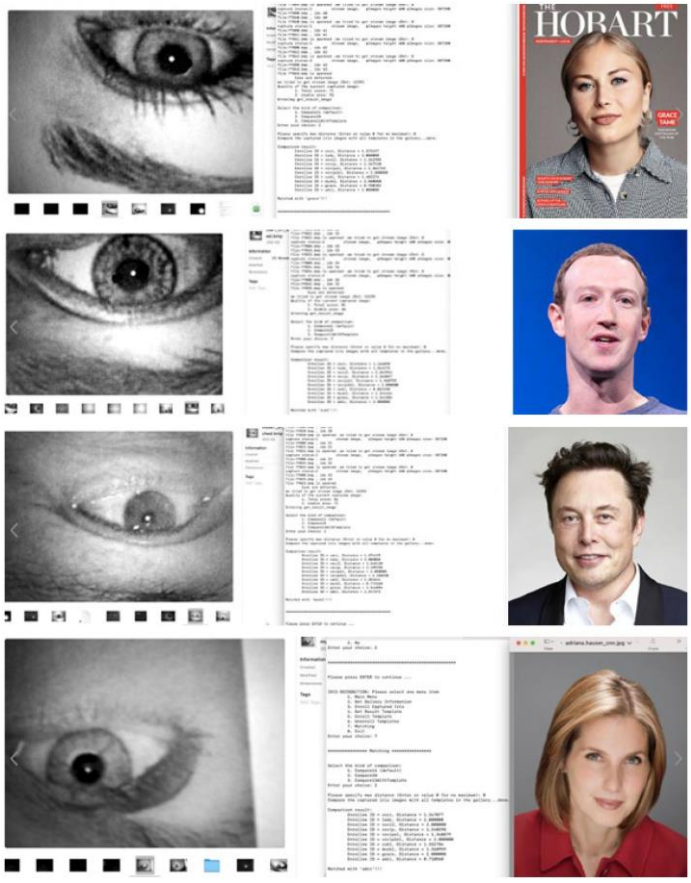


図 35：インターネットで露呈している肖像写真から収集した虹彩の登録と照合に成功した例（2 番目と 3 番目の肖像写真は、Wired[120]と Bloomberg[121]の画像をそのまま表示している）

[120] https://www.bloomberg.com/news/articles/2022-02-07/tesla-subpoenaed-by-sec-about-take-private-settlement-compliance#xj4y7vzkg

[121] https://media.wired.com/photos/5c54e3eca9851f2c3080460f/master/pass/FB-Oct2007-wi200710_101_pdf.jpg

画像クレジット：Wikimedia Commons

十分な解像度と品質を持つパターン情報の大部分は、登録と認識に成功することができました。図 35 に、収集した写真で登録と認識の両方に成功した例を示します。2 つのパターンは、距離がより厳密な閾値（0.8）をさらに下回っていました（0.71、0.77）。1 つはその閾値に近い距離（0.82）、もう 1 つは最大距離 1.0 を下回る距離（0.98）でした。

この実験では、リモート虹彩認証による生体認証システムに対する攻撃が可能であることが確認できました。リモート虹彩認証では、アカウントの作成もリモートから実行できます。

特定の人物の眼のパターンが特定の条件下で別の人物のものとして認識される可能性はあるのか?

答えは「可能な場合もある」です。投影する眼の画像を調整する今回の実験結果やベンダのセキュリティ閾値の実装具合に関する知識から言えるのは、発生頻度の少ないいくつかの条件下では可能であるということです。

図 36 のスクリーンショットでは、システムに未登録の虹彩パターンをシステムに登録済みのパターンの 1 つと照合した結果を確認できます。この結果において重要なことは、虹彩を収集するときの条件を意図的に低下させたということです。目は完全に開いておらず、わざと完璧ではない照明条件にしています。また、距離 0.96 は、ベースラインの実験で決めた閾値を下回っています。これは下図のスクリーンショットでも確認できます。トータルスコアは比較的低く、使用可能領域も虹彩が完全には見えていないことを示しています。

```
file:ff030.bmp , idx 30
file ff030.bmp is openned
        Eyes are detected.
we tried to get stream image iRet: 12293
Quality of the current captured image:
        1. Total score: 32
        2. Usable area: 43
Entering get_result_image

Select the kind of comparison:
        1. Compare11 (default)
        2. Compare1N
        3. Compare11WithTemplate
Enter your choice: 2

Please specify max distance (Enter or value 0 for no maximum
Compare the captured iris images with all templates in the g

Comparison result:
        Enrollee ID = lady, Distance = 1.341388
        Enrollee ID = zuk1, Distance = 1.239555
        Enrollee ID = musk1, Distance = 1.230378
        Enrollee ID = grace, Distance = 1.348928
        Enrollee ID = adri, Distance = 1.210109
        Enrollee ID = boti, Distance = 1.181434
        Enrollee ID = vovi, Distance = 1.342836
        Enrollee ID = vovi1, Distance = 1.175032
        Enrollee ID = vovi2, Distance = 1.203831
        Enrollee ID = vovi3, Distance = 0.966689
        Enrollee ID = glycedrop, Distance = 1.347872
        Enrollee ID = glycedrop2, Distance = 1.149981
        Enrollee ID = glueonsticknote, Distance = 1.253842
        Enrollee ID = vovi4, Distance = 1.216360
        Enrollee ID = vovi5, Distance = 1.200771
        Enrollee ID = vovi6, Distance = 1.216494
        Enrollee ID = deodrop, Distance = 1.278133
        Enrollee ID = foxi, Distance = 1.223609
        Enrollee ID = hase, Distance = 1.340965

Matched with 'vovi3'!!!
```

図 36：1 対多のテストにおけるシステムに未登録のパターンの認識結果

しかし、このセクションで調査したシナリオには、特に認証側から生体認証センサと環境条件を完全に制御することができない状況で、リモート生体認証を使用する実生活で起こりうるユースケースがあります。1 つの例が、ユーザが生体情報を使用してオンラインバンキングポータルでアカウントを認証する場合です。

ある画像のパターンを登録し、対応する実物の眼で認証することは可能なのか?

答えは「はい」です。実験では、印刷した研究者の眼の画像を使用してパターンを登録し、実物の眼のパターンと何とか一致させることに成功しました。

この実験では、紙に印刷した研究者の眼の画像を使用しました。実験を何度も繰り返して、収集に適した照明条件を見つける必要がありました。

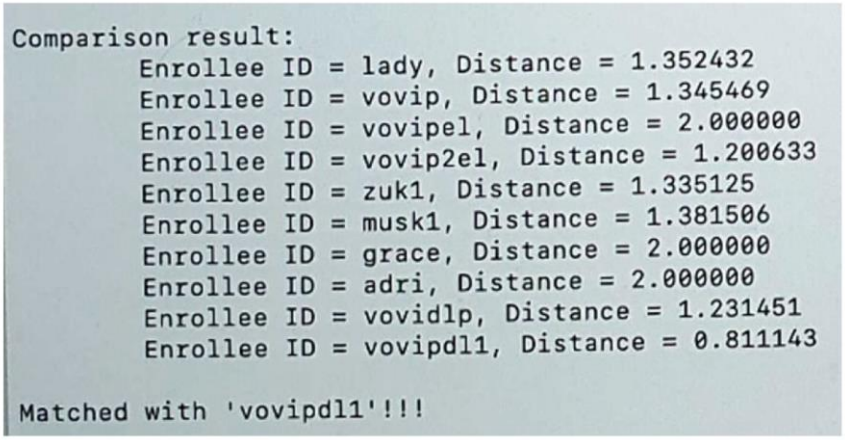


図 37：紙に印刷した画像から登録したパターンと実物の眼の照合

登録済みのパターンと収集した実物の眼の間の距離（0.81）は、実物の眼を登録して照合する場合と同等です。この攻撃の実行に成功した場合、登録目的で生体情報を提供したことがない人物のアカウントを作成するなど、攻撃者が別のシナリオを実行するのに役立つ可能性があります。

漏えいしたメディアを使用して人物を登録し、その人物の実物の眼で認証できる場合、恐喝や風評被害につながる可能性があります。攻撃者は、注目を集める人物（政治家、有名人、政府や企業のトップなど）がギャンブルやポルノなどの物議をかもす活動に加わっていた疑いがあると暴露することができます。この種の告発に偽造した生体情報の証拠を組み合わせた場合、その人物がこの疑惑に立ち向かうのは非常に困難である可能性があります。

さらに、ログイン日時および検証可能な生体パターンによる認証に成功したことに関連するログを示す（偽造された）データベースが意図的に漏えいすると、さらに困難になります。

実物の眼を登録し、画像のパターンと照合して認証することは可能なのか?

答えはおそらく「はい」です。白黒レーザプリンタで印刷したパターンを使用した実験では、成功に近い結果が得られました。

プリンタの解像度は、テストしていない他のフォトプリンタに比べて劣っていました。異なる条件下で同一人物を登録したパターンの場合に距離が最も近くなりました。ただし、距離1.18は1.0より大きく、したがって実験で1対多の本人確認が成功したと結果を判断するためにベースラインとして決定した閾値を上回っています。

```
Enrollee ID = lady, Distance = 2.000000
Enrollee ID = zuk1, Distance = 1.229158
Enrollee ID = musk1, Distance = 2.000000
Enrollee ID = grace, Distance = 1.231238
Enrollee ID = adri, Distance = 1.262931
Enrollee ID = boti, Distance = 2.000000
Enrollee ID = vovi, Distance = 1.351827
Enrollee ID = vovi1, Distance = 1.337057
Enrollee ID = vovi2, Distance = 1.207523
Enrollee ID = vovi3, Distance = 1.209559
Enrollee ID = glycedrop, Distance = 2.000000
Enrollee ID = glycedrop2, Distance = 1.333445
Enrollee ID = glueonsticknote, Distance = 2.000000
Enrollee ID = vovi4, Distance = 1.180270
Enrollee ID = vovi5, Distance = 1.207059
Enrollee ID = vovi6, Distance = 1.199296
```

図 38：印刷したパターンを実物の眼から登録したパターンに照合させる試み

今回の研究の主な焦点は露呈している生体データのリスクに関連することなので、将来の当社での研究で扱うこととし、ハードウェア虹彩センサを使用した実験はこの時点で終了することにしました。露呈している生体データが攻撃で使用されることやさまざまな生体認証センサに投影される可能性があることを証明するための十分な発見がすでに得られています。

また、多くのケースで普通の（近赤外ではない）カメラを使用したことを考えると、露呈している生体パターンの再利用はさらに容易になります。

TREND MICRO

〒151-0053

東京都渋谷区代々木 2-1-1　新宿マインズタワー

大代表 TEL：03-5334-3600 FAX：03-5334-4008

http://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。

Trend Micro Research