

Title	大阪大学における全学DX推進施策のリスクアセスメント : 顔認証入場システムのケース
Author(s)	岸本, 充生; 田中, 孝宣; 水町, 衣里 他
Citation	ELSI NOTE. 2024, 43, p. 1-21
Version Type	VoR
URL	https://doi.org/10.18910/95837
rights	
Note	

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University



大阪大学における 全学DX推進施策の リスクアセスメント： 顔認証入場システムのケース

Authors

岸本 充生	大阪大学 社会技術共創研究センター	センター長 (2024年6月現在)
田中 孝宣	大阪大学 社会技術共創研究センター	特任研究員 (2024年6月現在)
水町 衣里	大阪大学 社会技術共創研究センター	准教授 (2024年6月現在)
鈴木 径一郎	大阪大学 社会技術共創研究センター	特任助教 (2024年6月現在)
長門 裕介	大阪大学 社会技術共創研究センター	特任助教 (2024年6月現在)
カテライ アメリア	大阪大学 社会技術共創研究センター	特任助教 (2024年6月現在)
鹿野 祐介	大阪大学 COデザインセンター	特任助教 (2024年6月現在)
井出 和希	大阪大学 感染症総合教育研究拠点	特任准教授 (2024年6月現在)

※著者の一人である田中孝宣は、日本電気株式会社（NEC）から社会技術共創研究センター（ELSIセンター）に特任研究員として在籍出向している。本研究では ELSIセンターの立場からリスクアセスメントに参加した。また、NEC内においても大阪大学に顔認証技術を提供している部署とは直接の関わりはない。

目次

はじめに	3
1. 顔認証技術の適正利用に向けた産学共創研究.....	5
1.1. 顔認証技術の適正利用に向けた 10 の視点.....	5
1.2. リスクアセスメントフレームワークの開発	6
1.3. 顔認証技術を対象としたリスクアセスメントの特徴.....	8
2. 大阪大学における顔認証入場システムの概要.....	10
2.1. OUID システムの概要	10
2.2. 顔認証入場システム	11
2.3. データの処理.....	12
3. 大阪大学における顔認証入場システムについてのリスクアセスメントの実施	14
3.1. リスクアセスメントの実施要否.....	14
3.2. リスクアセスメントの対象	14
3.3. ステークホルダーの分析	15
3.4. リスクの洗い出し	15
3.5. 対策実施の前後のリスクアセスメント	17
おわりに	19

はじめに

大阪大学は2023年3月に、学内DX（デジタルトランスフォーメーション）の中枢を担う施策として、全学の学生および教職員を対象とした統合ID基盤「OUID(Osaka University IDentity)システム」を構築した。OUID推進室が中心となり、OUIDシステムを活用したアプリケーションの第1弾として、大学構内の屋内及び屋外の計27カ所に全学共通のインフラとして顔認証技術を活用した入場システムを設置・導入し、運用を開始しようとしている¹。これは2024年5月時点では、国内の大学で最大規模である。パーソナルデータを利活用する新しい技術を社会実装する際には、法令遵守に加えて、事前にプライバシー等への影響を含めた倫理的・社会的な課題を抽出し、可能な限り対策を実施しておくことが必要である。こうしたアプローチは「責任ある研究・イノベーション（Responsible Research and Innovation: RRI）」の実践であるともいえる²。

顔認証技術を活用した入場システムの導入は、パーソナルデータを利活用する新しい技術の社会実装であり、新規技術の倫理的・法的・社会的課題（ELSI）を含みうるものである。そのため当該システムの運用開始前には、大学内の構成員である学生および教職員だけでなく、来訪者等も含めた関係者へのありうるリスクを事前に把握する必要がある。加えて実施主体は、これらのリスクについて、許容できないリスクがないと考えられるレベルまで対策を講じ、そのことをわかりやすくステークホルダー（影響を受ける可能性のある主体）に向けて説明し、またステークホルダーの声を取り入れながら、システムを運用・改善していく必要がある。しかしながら、これらのリスクアセスメントを実施主体単独で行うことには困難を伴うケースが少なくない。

大阪大学は2020年4月に、新規技術の社会実装に向けた課題に取り組むための組織として、社会技術共創研究センター（以下「ELSIセンター」）を設置した。ELSIセンターでは、学内及び学外の様々なステークホルダーと連携しながら、多様な新規技術の倫理的・法的・社会的課題（ELSI）についての実践研究を実施している。以上のような背景から、大阪大学ELSIセンターでは、第三者的な立場からOUIDシステムを活用した顔認証技術の導入についてのリスクアセ

¹「大阪大学とNEC、学生・教職員・卒業生などの統合ID基盤を構築 2024年4月から世界No.1の顔認証技術を活用した入場管理を国内大学最大規模で導入 数十万人のIDを一括管理し、各種システム・サービスと連携」（2023年12月11日）https://www.cmc.osaka-u.ac.jp/wp-content/uploads/2023/12/20231211_01.pdf

²JST-CRDS『ELSIからRRIへの展開から考える科学技術・イノベーションの変革—政策・ファンディング・研究開発の横断的取り組みの強化に向けて—』（2022年3月）<https://www.jst.go.jp/crds/report/CRDS-FY2021-RR-07.html>

メントの実施に関わることとなった。

本レポートは、その実施結果を学内関係者と共有するとともに、多様なステークホルダーとの対話を促すことで、OID システムのみならず、同様のシステムが大学をはじめとするさまざまな組織に導入される際に、同様の取り組みがおこなわれることが必要になるであることを考慮し、公表するものである。

第 1 章では背景情報として、ELSI センターが日本電気株式会社（NEC）と実施している「顔認識技術の社会実装における社会技術の研究」の成果である「顔認証技術の適正利用に向けた 10 の視点」（以下「10 の視点」）と「リスクアセスメントフレームワーク」を紹介する。第 2 章では本レポートの議論の中心となる大阪大学における顔認証入場システムの概要を示す。第 3 章では第 2 章で紹介した大阪大学における顔認証技術の導入を対象としたリスクアセスメントについて、実施の要否、アセスメントの対象、ステークホルダーの分析、リスクの洗い出し、対策前後のリスクアセスメントというプロセスを順に追っていく。最後に、本レポートで示した取り組みの到達点と限界、今後の見通しを示す。

1. 顔認証技術の適正利用に向けた産学共創研究

1.1. 顔認証技術の適正利用に向けた 10 の視点

大阪大学 ELSI センターは、OUID システムを活用した顔認証技術の導入が検討される文脈とは独立して、2022 年 7 月から日本電気株式会社（以下「NEC」）と顔認証技術を題材とした倫理的・法的・社会的課題(ELSI)に関する共同研究を実施している³。本共同研究は、長年、顔認証技術を活用した事業を推進してきた NEC の知見と、新規科学技術に係る ELSI やガバナンスのあり方などの研究活動における大阪大学 ELSI センターの知見を組み合わせ、共同で進めるものである。顔認証技術を活用するサービスの事業構造は複数存在するが、主に対象としているのは、顔認証技術そのものをサービス事業者提供するプロバイダー事業者と、顔認証技術を活用している各種サービスを利用者に直接提供するサービス事業者（ないしデプロイヤー）という事業構造である。

このような事業構造を持ついくつかの具体的な顔認証技術の適用事例を用いた ELSI 検討を通して、2023 年 3 月には、顔認証技術を多様な適用先に社会実装するための事業開発ガイドとして、以下に示すような「顔認証技術の適正利用に向けた 10 の視点」を策定した⁴。NEC 社内向けにはさらに、視点ごとに、それぞれの視点を実践するために必要な複数の論点が用意されている。

< 10 の視点 >

視点 1. 顔認証技術を使う必要性があるか。

視点 2. 取得するパーソナルデータは必要最小限であるか。

視点 3. 取得するパーソナルデータの処理プロセスをプロバイダー事業者、サービス事業者およびステークホルダーが把握しているか。

視点 4. サービスの精度や生じるかもしれない偏り(バイアス)を把握しているか。

³ 「NEC と大阪大学社会技術共創研究センター、顔認証技術を題材とした倫理的・法的・社会的課題(ELSI)に関する共同研究を開始～先端技術が Well-being に寄与するイノベーションモデルの構築を目指す～」(2022 年 9 月 12 日)
https://elsi.osaka-u.ac.jp/system/wp-content/uploads/2022/09/PR_NEC_ELSI_20220912.pdf

⁴ 「大阪大学 ELSI センターと NEC、顔認証技術の適正利用に向けたガイドおよびリスクアセスメント手法を策定」(2024 年 5 月 9 日)
https://resou.osaka-u.ac.jp/ja/research/2024/20240509_4

- 視点 5. 顔認証が誤った場合に利用者に大きな不利益が生じないように配慮されているか。
- 視点 6. 顔認証技術を使えない人/使いたくない人を公平に扱う仕組みになっているか。
- 視点 7. 利用者本人が納得してサービスを利用していると確信できるか。
- 視点 8. 顔認証および他サービスとの連携により、意図しない影響が生じないか検討されたか。
- 視点 9. 利用者および社会へのリスクと対応に関して、プロバイダー事業者とサービス事業者との対話が適切になされているか。
- 視点 10. 運用開始後の事後検証が想定されているか。そのような仕組みがあるか。

1.2. リスクアセスメントフレームワークの開発

上記の「10 の視点」はある種のチェックリストとして用いることもできるが、これらの問いかけは Yes/No の二分法で単純に答えられるものばかりではない。顔認証技術を使う必要性があるならば、完全な Yes と完全な No の間を、できるだけ Yes に近づけていくというアプローチが必要となる。そのためには「リスク」概念が有用である。リスク概念を用いることで、完全な Yes と完全な No の間のグラデーション部分を定量的・定性的に表現することができる。

つまり、先に挙げた「10 の視点」を参考に、潜在的なリスク項目を洗い出し、それら 1 つ 1 つについて、Yes と No の間を何段階かで評価したうえで、必要に応じてリスク削減対策を実施することで、どのリスクについて、どの程度、完全な Yes に近づけているかを可視化することができる。共同研究においては、そのような形で、顔認証技術を活用した製品やサービスを、適切に社会実装するために必要なリスクアセスメント手法を開発し、2023 年 12 月にプロトタイプを完成させた。

本リスクアセスメント手法は、図 1 のように、ELSI の観点を取り入れたリスクアセスメントの枠組みであり、諸外国において主に公的機関のパーソナルデータ利活用の場面において実践されてきたプライバシー影響評価（PIA）にも活用できる⁵。本リスクアセスメント手法は、国際

⁵ 諸外国におけるプライバシー影響評価（PIA）の制度化の概観については、岸本充生「パーソナルデータ利活用のためのリスクマネジメント（1）：プライバシー影響評価（PIA）の制度化」, ELSI NOTE 39 1-26 2024 年 4 月 を参照。 <https://doi.org/10.18910/94924>

標準化機関（ISO）と国際電気標準会議（IEC）が策定したPIAの規格（ISO/IEC 29134:2023）⁶を参考にしており、また本規格の枠組みはより一般的なリスクマネジメント規格に基づいている⁷。すなわち、データ利活用のライフサイクルに沿ってステークホルダーを可能な限り広く想定したうえで「守りたいもの」を列挙し、それらへの影響として発生しうるリスクを洗い出す。多様なステークホルダーの多様なリスクを洗い出すためには、多様なバックグラウンドを持つ者が集い、創発的な意見交換を通じて実施することが望ましい。そこで挙げられた数多くのリスクを、類似のものはまとめて、リスク項目として整理するまでが「リスク特定」である。続いて、何も対策を実施しない状態でのリスクの大きさを、リスク項目ごとに推定する（「対策前のリスクアセスメント」）。その結果をリスクマップに並べ、リスク対応方針を確認したうえで、何もしないことを含めた「リスク対策オプション」を挙げ、最適な対策を選択する。対策後にも残る残余リスクを推計し（「対策後のリスクアセスメント」）、そのレベルが一般的に許容できないものがないと判断できることを確認する。さらに、プロジェクトの実施後には事後評価を実施することになる。図1にこれらのプロセスを整理した。

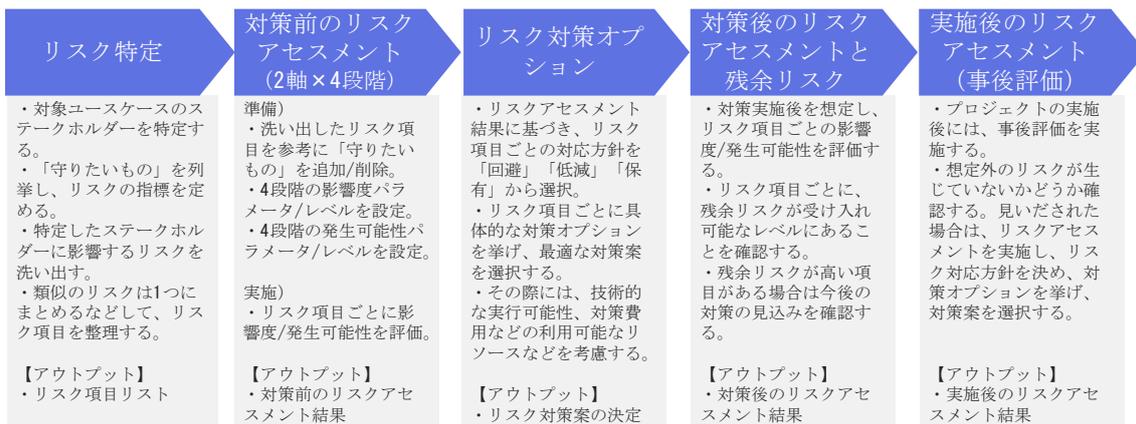


図1. リスクマネジメントの全体プロセス

⁶ ISO/IEC 29134:2023. “Information technology — Security techniques — Guidelines for privacy impact assessment” (Edition 2, 2023).

⁷ ISO 31000:2018. “Risk management — Guidelines” (Edition 2, 2018).

1.3. 顔認証技術を対象としたリスクアセスメントの特徴

顔写真のようなパーソナルデータの利活用を対象としたリスクアセスメントは、化学物質曝露の健康リスクアセスメントや工学的な事故リスクアセスメントなどと異なり、ステークホルダーが多く、リスクの種類も多様、かつ、プライバシーや人権といった定量化しづらいリスクも少なくない。また、リスクの見積もりにおける「正しさ」の考え方も、ステークホルダーにより大きく異なる。つまり、顔認証技術を対象としたリスクアセスメントでは、誤認証率など、データに基づいて判断できる部分もあるものの、利用者がどう行動するか、どう反応するか、どう感じるかといった部分は、客観的な正しさを議論することが難しい。すなわち、リスクを特定することにも、リスクアセスメントすることにも独特の難しさが存在する（図2）。

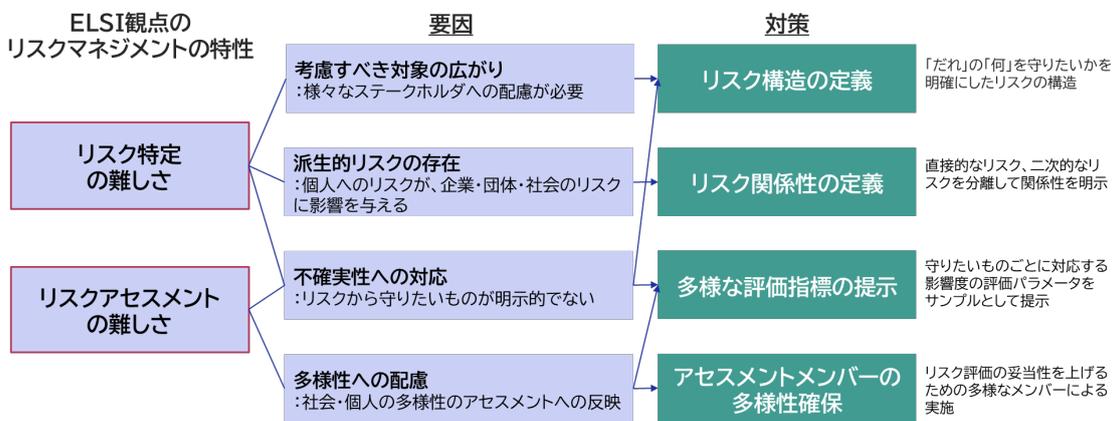


図2. 本リスクアセスメントフレームワークの特徴

そのため、まずは「誰にとってのリスクか（ステークホルダーは誰か）」「どんな種類のリスクか（守りたいものは何か）」を明示的に検討することから始めた。

ステークホルダーは、第一義的には顔認証システムの利用対象者である。しかし、場合によっては、サービス事業者のレピュテーションや社会全体への影響といった二次的・派生的なリスクも考慮する必要がある。そのため、両者を明示的に区別し、両者の関係性を明記することとした。守りたいものは、利用者の健康・安全や財産といった客観的に評価できるものだけでなく、嫌な思いをするといった主観的なものも含めて、ステークホルダーの多様性及び多様な価値観を組み込んだ評価指標を用意することを目指した。事業者が社内向けにリスクアセスメントを実施する場合などは、守りたいものに、事業者の信頼や評判といったものも含まれる。しかし、本レポートでは、レピュテーションを含めた二次的・派生的なリスクについては明示的には取り上げないこととした。

また、リスクの大きさは「影響度」と「発生可能性」の二軸で評価し、それぞれを4段階ずつで見積もった（図3）。影響度については、無視可(1)、限定的(2)、重大(3)、甚大(4)の4段階、発生可能性については、非常に低い(1)、一定の可能性(2)、ある程度高い(3)、非常に高い(4)の4段階で見積もった。リスクの大きさは両者を掛け合わせた数値とし、最小が1、最大が16となる。また、リスク対応方針は、回避、低減、保有の3種類とした。これらの結果は図4のような「リスクマップ」として示される。縦軸に「影響度レベル」、横軸に「発生可能性レベル」をとり、リスク項目ごとにマッピングする。そのうえで、リスク対応方針としては、リスクの大きさが8以上では必ず対策をとるべき（「回避」）、6以下では可能な限り対策をとるべき（「低減」）、2以下なら必ずしも対策をとる必要はない（「保有」）とした。

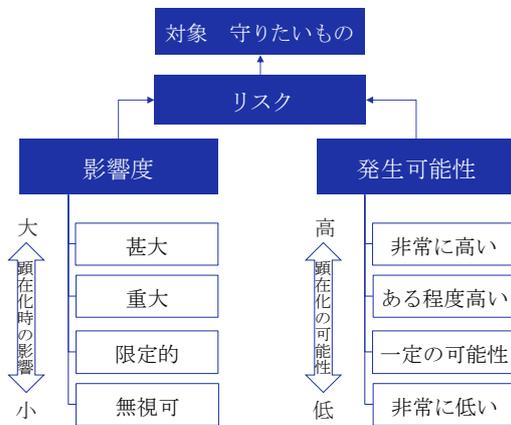


図3. リスクの大きさの見積もり方法

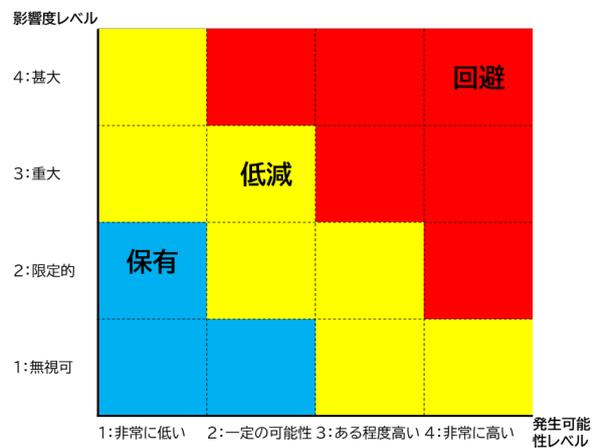


図4. リスクマップとその使い方

表1には利用者に対する「守りたいもの」とその影響度パラメータ、発生可能性パラメータとそれぞれの具体的な指標例を挙げた。顔認証技術の適用場面によっては該当しない項目もあるし、追加すべき項目がある可能性もある。また、リスクアセスメントの実施前に、影響度と発生可能性、それぞれの4段階についてあらかじめ目安を定めておくと点数がつけやすく、関係者間での合意が得やすい。しかし、目安については、顔認証技術の適用ケースごとに異なってくるため、すべてに適用可能な普遍的なスケールを定めることは難しい。

表1. 守りたいものと影響度・発生可能性のパラメータの例

守りたいもの	影響度	発生可能性
	パラメータ	パラメータ
健康、安全	身体的影響	件数/件数比率
財産	経済的影響	件数/件数比率
人権、プライバシー	社会・精神的苦痛	人数/人数比率
尊厳	実存・精神的苦痛	人数/人数比率
自由、自律	行動萎縮の度合い	人数/人数比率
	意思決定への影響	
時間、機会	機会損失の程度	利用回数に対する比率
利便性、期待	がっかり、期待外れ	人数/人数比率
対人関係	交友関係への影響	人数/人数比率

このような作業は、多様なバックグラウンドを持つ複数のメンバーで実施することにより、これまで扱いが難しかった人権やプライバシー、人としての尊厳、自由などに関連するリスクについてアセスメントを行うことができるようになる。

ここまでは、大阪大学 ELSI センターと NEC が、顔認証技術を題材とした ELSI に関する共同研究を通じて開発した顔認証技術を対象としたリスクアセスメント手法の概要について記述してきた。これらを踏まえ、第2章以降では、この手法を大阪大学における顔認証入場システムの導入に適用したケースを紹介する。

2. 大阪大学における顔認証入場システムの概要

2.1. OUID システムの概要

大阪大学では中期経営計画で掲げる「OU マスタープラン 2027」の一環として、2022年4月に OUDX 推進室を立ち上げ、学内の DX を推進している。その DX 施策の中核を担う施策として、入学前や卒業後・退職後を含めた生涯にわたる ID 活用を想定し、大阪大学に関わるすべての構成員（大阪大学コミュニティ）の統合 ID 基盤として、クライアント証明書による認証機能を持つ OUID システムを 2023年3月に構築している。このシステムに基づいて、大阪大学コミュニティに存在するすべてのステークホルダーに対し、学内外に対して付加価値の高いサービスを

提供する「OUID サービス構想」の実現を目指すとしている⁸。

2.2. 顔認証入場システム

大阪大学では 2023 年 4 月からは、OUID システムと連携した各種システムの開発・導入へと発展させていくためのフェーズに入っており、その最初に導入されようとしているのが、顔認証入場システムである。このシステムは、ELSI センターの共同研究先でもある NEC が提供するクラウドサービス「Bio-Idiom Services ID 連携」を利用したものである。

顔認証入場システムの導入の背景として、大阪大学では、建物や部屋ごとにシリンダーキーや IC・磁気カードなど、入場管理の方法が異なっていたことに加え、紛失ケース・磁気喪失ケースの多さや、手書きの鍵貸出台帳の準備や記入といった煩雑な手続きが大きな事務負担となっていたことが挙げられる。

そのような課題の解消を目的として、構成員に一意に割り当てられた OUID と連携した顔認証入場システムを導入することが現在計画されている。これらの仕組みは、採用・退職・配置転換等の人事異動と自動連動させることも可能である。ただし、顔認証入場システムを利用するかどうかは任意であり、従来のカードキーを使い続けることも可能である。

⁸「大阪大学と NEC、学生・教職員・卒業生などの統合 ID 基盤を構築 2024 年 4 月から世界 No.1 の顔認証技術を活用した入場管理を国内大学最大規模で導入 数十万人の ID を一括管理し、各種システム・サービスと連携」(2023 年 12 月 11 日) https://www.cmc.osaka-u.ac.jp/wp-content/uploads/2023/12/20231211_01.pdf

顔認証入場システムは、2024年6月から試行導入が予定されており、大阪大学内に、吹田キャンパスの本部事務機構棟をはじめとするその他建物含め計27カ所に設置されている。図5の写真はその中の1つである。



図5. 吹田キャンパスのサイバーメディアセンター本館入口に設置している顔認証カメラ

2.3. データの処理

本人が希望し、顔認証による入場を利用するためには、あらかじめ顔写真データをアップロードしておく必要がある。利用者は専用ウェブサイトアクセスし、プライバシーポリシーを読み、その内容に同意したうえで顔写真をアップロードする。その際は、顔写真以外にも、本人が大学に所属していることを示す各種個人情報を入力する必要がある。アップロードされた顔写真データは、大阪大学内のサーバと NEC のクラウド「Bio-IDiom Services ID 連携」に保管され、入場の顔認証を含む ID 照合用に利用される。顔認証による入場は、カメラの前の顔映像から得られた特徴量データが、あらかじめアップロードされた顔写真の特徴量データと照合さ

れ、特徴量の一致度を表す照合スコアが閾値を超えたら本人であると確認され開錠される。ただし、入場の際に撮影された顔写真はその場での照合のためのみに用いられ、2週間程度で破棄されることになっている。そのため、顔写真そのもの、あるいは他のデータと組み合わせられて分析されたり、二次利用されたりすることは想定されていない。

3. 大阪大学における顔認証入場システムについてのリスクアセスメントの実施

3.1. リスクアセスメントの実施要否

リスクアセスメント自体にも一定の時間と費用がかかることから、システムの導入前にその実施の必要性の判断を行うことが求められる。リスクが極めて小さい、あるいは、既存のシステムとほとんど変わらないような場合は、リスクアセスメントは必要ないという判断がなされる。このプロセスは、プライバシー影響評価（PIA）では通常、閾値分析（threshold analysis）と呼ばれる。

顔認証入場システムは大阪大学にとって新規の導入であること、顔写真という比較的センシティブな個人情報を利用すること、大阪大学に所属する学生および教職員に加え、契約業者等の多様なステークホルダーが訪れる大学構内で広く運用されることなどから、リスクアセスメントの実施が必要であることが想定された。

大阪大学 ELSI センターでは、顔認証入場システムを運用する大阪大学 OUDX 推進室（以下「OUDX 推進室」）からの依頼を受け、センター内で検討した結果、完全な形でのリスクアセスメントの実施が必要であると判断し、第三者的な立場から OUID システムを活用した顔認証技術の導入についてのリスクアセスメントを実施することとなった。本リスクアセスメントには、倫理学、社会学、経済学、理工学、農学、薬学等の多様なバックグラウンドを持つ ELSI センターのメンバー（以下、「参加メンバー」）が参画した。リスクアセスメントの進め方として、前述の「10 の視点」と「リスクアセスメントフレームワーク」を活用し、OUDX 推進室へのヒアリングを重ねながら、アセスメント対象の選定、ステークホルダーの分析、リスクの特定、対策実施前のリスクアセスメント、リスク対策オプションと対策案の決定、対策実施後のリスクアセスメントと残余リスクの確認を実施した。

3.2. リスクアセスメントの対象

リスクアセスメントの対象は、2024 年 6 月から試行導入を予定している計 27 カ所に設置された顔認証入場システムとした。OUID サービスの顔認証技術の活用としては、入場のほかに、図書館の本の貸出・返却や授業の出欠管理等へサービス拡大を検討している。しかし今回のリスクアセスメントではこれらは対象外とし、今後、新しい機能が実装される場合には、それぞれ閾値分析を行い、必要だと判断されれば同様のリスクアセスメントを実施することを想定し

ている。また、サイバーセキュリティ面のリスクに関しては別途対策が取られているため本リスクアセスメントでは対象外とした。

3.3. ステークホルダーの分析

評価対象となる顔認証入場システムのステークホルダー（影響を受ける可能性のある主体）を特定するために、大学に出入りする関係者の属性を洗い出した（図6）。学内関係者としては、顔認証入場システムの主な利用者である学生、教員、職員が挙げられる。そのほか、キャンパス内には大学構内の保育園に通う園児とその保護者、食堂や売店の従業員も存在する。また、関連する属性としては、システム管理者としての OUDX 推進室および部局ごとの管理者も挙げられる。学外関係者には、他大学の学生や教員、企業や行政などの他組織からの訪問者に加えて、大学構内に入出入りする契約業者、周辺住民、受験生、吹田キャンパス構内にある大阪大学附属病院（医学部と歯学部）の患者および患者の家族等が挙げられる。また、国外からの訪問者も存在する。このようなステークホルダー分析の結果を潜在的なリスクの特定に活用する。

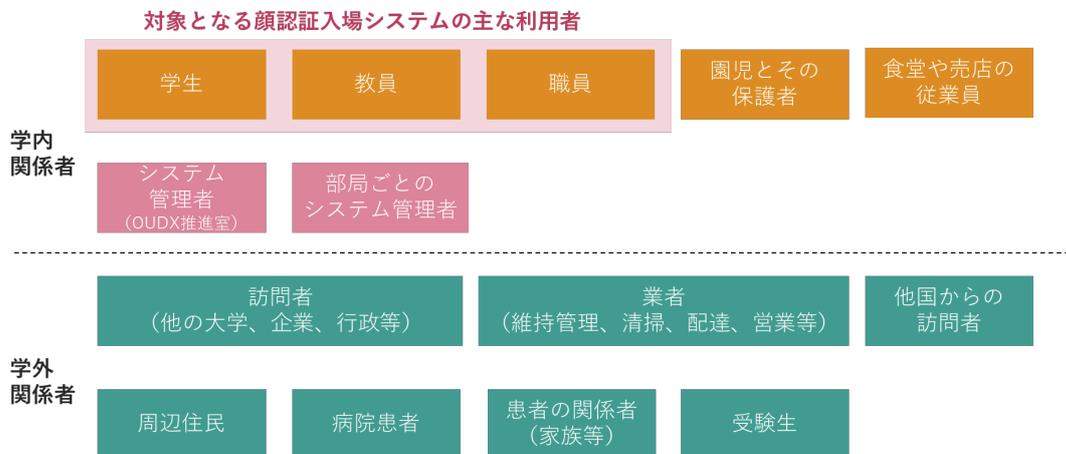


図6. 顔認証入場システムのステークホルダー分析

3.4. リスクの洗い出し

リスクの特定については、ELSIセンターからの参加メンバー各々が「10の視点」を参考にしつつ、想定されるリスクの洗い出しを行った。リスクの洗い出しを行う際は、リスクの内容と併

せて、影響を受ける対象、対象者が守りたいものを明示するようにした⁹。結果、計 57 件のリスクが特定された。これをたたき台とし、メンバーが集まって協議し、類似のリスク項目を集約する作業を通して計 13 件のリスク項目に整理された（表 2）。表 2 の「件数」列は、最初に挙げられたリスクの数を示しており、3 番目の「内容面のコミュニケーションの課題」に含まれるものが多かったことが分かる。これらは顔画像が分析されたり、大学から監視されたり、他のデータと連携されたりするのではないか、顔認証による入場以外の手段がなくなったのではないかといった懸念や、顔認証の利用対象でないが大学に出入りする人々からのとまどいなど、説明が足りないことや説明へのアクセスの困難による懸念や不安としてまとめたものである。

⁹それぞれのリスクについて、サービス事業者（NEC）や大阪大学への影響についても検討したが本レポートでは取り上げない。

表2. 抽出されたリスク項目リスト

No.	リスク項目	件数	内容
1	データの過剰収集・保存	1	目的に対して必要最小限を超えるデータの取得・保存による情報漏洩時の被害
2	プロセス面のコミュニケーションの課題	1	ステークホルダーからの意見を聞いたり、事前の説明をしたりすることなしに導入したことへの不満
3	内容面のコミュニケーションの課題	21	説明不足や説明へのアクセスの困難による誤解や不安 - 取得データの目的外利用への懸念 - 顔認証を強制している（代替手段がない）という誤解 - 監視されているのではないかという懸念 - 学生や教職員以外の関係者からの戸惑いや不満
4	公的機関への情報連携に関する不安	2	公的機関への情報提供の方針が不明確 - 事件・事故にあった場合の懸念
5	ユーザビリティの課題	3	顔情報の登録、変更、削除のしにくさ
6	アカウントビリティの課題	6	サービスのライフサイクル（導入、変更、終了）を通じた正当性の不足 - 他大学との方針の違いによるトラブルの可能性
7	誤認証	8	誤認証時の不利益 - 本人拒否：会議/授業の欠席、代替手段による手間 - 他人受入：意図しない不正アクセス
8	包摂性の課題	6	使えない人や使いたくない人の不利益 - 日本語が分からない人の理解不足 - 視覚障害者等への配慮不足 - 一時的に使いたくない人への対応
9	なりすまし	3	登録時や運用時に他人になりすまして登録・利用
10	迷惑行為	2	顔認証サービスの想定外の迷惑行為 - 変顔で遊ぶ等
11	事後検証の欠落	3	運用後の実態把握の仕組みの欠如 - 利用者の不満等の実態を把握できない
12	写り込み	1	顔認証時の第三者の写り込み
13	有効でない同意	1	顔認証サービスへの不本意な同意 - 利用を推進する職場での同調圧力

3.5. 対策実施の前後のリスクアセスメント

リスクアセスメントの結果の示し方として、影響度と発生可能性の二軸からなる4×4のリスクマップを用いることとした。影響度と発生可能性を1から4でそれぞれ点数化し、その積をリスクレベルとした。リスクの大きさは、従来から用いられているカードキーによる入場を継続して利用できることを前提に、合理的に考えられる最悪のケースについて、参加メンバーで様々な可能性を協議した上で点数化を行った。例えば、人権・プライバシーについては表3のような目安を設けた。

表3 影響度と発生可能性のレベルの目安

影響度	指標	甚大	重大	限定的	無視可
	精神的な苦痛	回復不可能なダメージ	治療が必要なダメージ	一時的なダメージ	軽微な不快感
発生可能性	指標	非常に高い	ある程度高い	一定の可能性	非常に低い
	人数比率	50%以上	10%以上	1%以上	1%未満

リスクアセスメントの結果、対策必須が4件、可能な限り対策すべきが8件、対策任意は1件となった。これらの結果は図7の左に示した。続いて、OUDX 推進室に実施済みの対策をヒアリングした上で、リスク項目ごとに追加すべき対策案を参加メンバーで検討した(表4)。

そのうえで、検討した対策案を全て実施した場合のリスクアセスメント、すなわち対策実施後のリスクアセスメントを行った。その結果、対策案を実施することで発生可能性あるいは影響度、またはその両方が低下し、全てのリスク項目が対策任意、もしくは可能な限り対策すべきになっていることが確認できた(図7の右)。例えば、学内説明会を実施することで、対策実施前リスクの高かった②(プロセス面のコミュニケーションの課題)や⑬(有効でない同意)のリスクが大きく削減されることが分かる。また、ログ保存期間の適正化により①(データの過剰収集・保存)のリスクが、現地掲示文や救済手段(現行カードの利用継続)により⑦(誤認証)のリスクが削減されることが分かる。

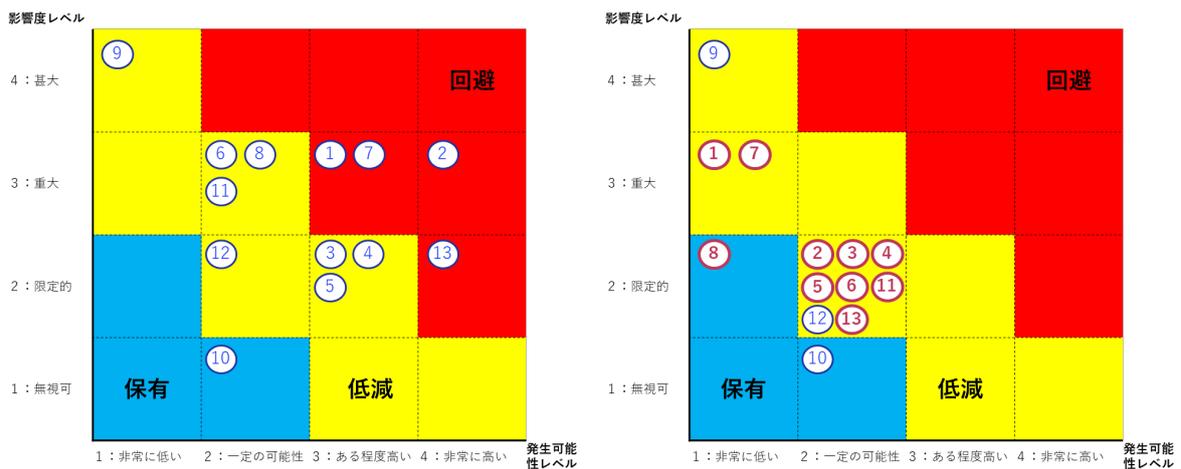


図7. リスクアセスメント結果(左が対策実施前、右が対策実施後)

※図中の番号は表2の1列目の番号のリスク項目を表している。

表4 特定したリスク項目を基に検討した対策案

No.	対策案	関連する リスク項目No.
A	【ログ保存期間の適正化】 顔認証で入場した際のログ保存期間を最小限にする。	1
B	【学内説明会】 対象となる組織に対し、事前に説明会を開催する。後日、動画を視聴可能にする。	2, 3, 4, 6, 13
C	【ポータルサイト開設】 顔認証入場システムについて理解を促すためのポータルサイトを開設する。	2
D	【事前の意見収集および対話】 利用者含む関連ステークホルダーと事前に対話し、意見を収集する。	2
E	【問合せ窓口設置】 顔認証入場システムについて問合せを受け付ける窓口を設置する。	2, 6, 11
F	【プライバシーポリシーの提示】 顔認証入場システムのプライバシーポリシーを提示する。	3, 4
G	【現地掲示文】 顔認証カメラを設置している場所に、カメラの利用目的と問い合わせ先を記載した資料を掲示する。	3, 7
H	【操作マニュアルの提示】 顔認証入場システムを登録/利用するための操作マニュアルを提示する。	5
I	【救済手段】 顔認証入場システムが正常に動作しない場合の救済手段として現行のカードキーを利用可能にする。	7, 9
J	【ユニバーサルデザイン】 日本語が分からない人への配慮：プライバシーポリシー等の重要情報は英語版も用意する。 顔認証を使えない人/使いたくない人への配慮：代替手段として現行のカードキーを利用可能にする。	8
K	【登録時の第三者確認】 顔画像を登録する際のなりすましを防ぐため、第三者が確認するプロセスを組み込む。	9
L	【人事評価との切り離し】 サービスの登録率および利用率を組織KPIに設定することを禁止する。	13

以上のリスクアセスメントの結果から、対策を講じることによって利用者に対する潜在的なリスクを削減することが可能であり、顔認証入場システムの導入には、大学としておおむね許容できないリスクはないであろうことを確認した。もちろん、リスクの洗い出しやリスクレベルの評価には参加メンバーの想像力の範囲という限界が存在するため、利用開始後に利用者からのフィードバックを十分に取り入れた事後検証が不可欠である。

おわりに

今回は大阪大学のキャンパス内の一部に2024年6月から試行導入される顔認証入場システムを対象に、導入前の段階でリスクアセスメントを実施し、利用対象者に関する、個人情報の取扱い・プライバシー保護の観点を中心としたリスク項目を洗い出し、対策実施後のそれらのリスクレベルは、大学として導入するにあたり、許容できないリスクレベルにはないであろうことを確認した。ただし、すべてのリスクが洗い出せたと言い切れるわけでもなく、また、抽出し

たリスクの残余リスクはゼロではないこと（図7）、ステークホルダーのリスクに対する感受性にはばらつきがあり感度の高い人もいること、などを考えると、図1のリスクマネジメントの全体プロセスにも記載した通り、実施後のリスクアセスメント（事後評価）を実施することは必須であろう。このような情報技術を対象としたリスクアセスメントは、プライバシー影響評価（PIA）として諸外国では主に公的機関の取り組みを対象に実施されてきたが、方法論が必ずしも確立されているとはいえず、実践を通して、リスクアセスメント手法の一般化・標準化も進めていく必要がある。

加えて今後も OUID サービスにおいて顔認証技術を活用した新たなサービスの導入が検討されているため、導入前の段階において、リスクアセスメントの実施の必要性を適宜検討する等、適切な対応をしていくことが必要となる。また、それに限定せず、想定外のリスクが顕在化していないかどうか常に注意を払い、定期的にステークホルダーからのフィードバックを得るように努めることを推進主体には求めたい。

大学や企業、また自治体でも、デジタルトランスフォーメーション（DX）が進められており、顔認証技術以外にも様々な新規技術の実装が試みられている。特にパーソナルデータを利活用するような先進的な技術・サービスでは、どういうデータを利用するか、どのようなアルゴリズムを使っているか、分析結果をどのように適用するのか、どのようなプロセスで進めるのか等、様々な意思決定が必要となる。これらには 1 つだけの正解があるわけではなく、適切に導入するには「リスクに基づくアプローチ（risk based approach）」の適用が必要不可欠となると考えられる。本レポートで紹介したケースが参考となれば幸いである。

ELSI NOTE No. 43

令和 6 年 6 月 5 日

大阪大学における全学 DX 推進施策のリスクアセスメント： 顔認証入場システムのケース

岸本 充生	大阪大学 社会技術共創研究センター	センター長 (2024 年 6 月現在)
田中 孝宣	大阪大学 社会技術共創研究センター	特任研究員 (2024 年 6 月現在)
水町 衣里	大阪大学 社会技術共創研究センター	准教授 (2024 年 6 月現在)
鈴木 径一郎	大阪大学 社会技術共創研究センター	特任助教 (2024 年 6 月現在)
長門 裕介	大阪大学 社会技術共創研究センター	特任助教 (2024 年 6 月現在)
カテライ アメリア	大阪大学 社会技術共創研究センター	特任助教 (2024 年 6 月現在)
鹿野 祐介	大阪大学 CO デザインセンター	特任助教 (2024 年 6 月現在)
井出 和希	大阪大学 感染症総合教育研究拠点	特任准教授 (2024 年 6 月現在)

Risk assessment of OUID(Osaka University IDentity) system: Case of facial recognition entrance system

Atsuo Kishimoto	Osaka University
Takanori Tanaka	Osaka University
Eri Mizumachi	Osaka University
Keiichiro Suzuki	Osaka University
Yusuke Nagato	Osaka University
Amelia Katirai	Osaka University
Yusuke Shikano	Osaka University
Kazuki Ide	Osaka University



大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

〒565-0871 大阪府吹田市山田丘 2-8
大阪大学吹田キャンパステクノアライアンス C 棟 6 階
TEL 06-6105-6084
<https://elsi.osaka-u.ac.jp>

 **大阪大学**

Osaka University
Research Center on
Ethical, Legal and
Social Issues