2024年6月21日　第37回日本リスク学会春季シンポジウム

リスクアセスメント事例
～大阪大学の顔認証入場システム～

特任研究員　田中孝宣

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

NEC

Osaka University
Research Center on
Ethical, Legal and
Social Issues

目次

1. 大阪大学ELSIセンターとNECの共同研究成果
   （ELSI観点を組込んだリスクアセスメント手法）

2. 大阪大学の顔認証入場システム

3. リスクアセスメント

１．大阪大学とNECの共同研究成果

ELSIセンターとNECの共同研究を2022年より開始。顔認証技術の適正利用に向けたガイド「10の視点」およびELSI観点を組込んだ「リスクアセスメント手法」を策定。

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4月よりNECにおける顔認証事業で検証開始

2024-5-9 ● 工学系

社会技術共創研究センター／データビリティフロンティア機構　教授　岸本　充生

研究成果のポイント

- ELSIセンターとNECは、共同研究を通じ、顔認証技術の適正利用に向けたガイド「顔認証技術の適正利用に向けた10の視点」および「リスクアセスメントフレームワーク」を策定。
- 「顔認証技術の適正利用に向けた10の視点」：顔認証技術を活用した事業の社会受容性向上に向けた取り組みにおいて留意すべき事項を整理した事業開発ガイド。事業開発の企画・開発・運用のフェーズごとのチェックリスト、リスクアセスメントに活用可能。
- 「リスクアセスメントフレームワーク」：ELSIの観点を取り入れたリスクアセスメントの枠組み。顔認証技術を採用することによる人権・プライバシーやレピュテーションに関連するリスクについて、適切なアセスメントを行うことが可能に。
- 今後も、共同研究を通じて、ELSIに配慮した事業開発の標準プロセスなどの研究・策定に取り組む。

<https://resou.osaka-u.ac.jp/ja/research/2024/20240509_4>

１．大阪大学とNECの共同研究成果：10の視点

顔認証技術を保有するプロバイダー事業者が、サービス事業者を通して利用者にサービスを提供する事業構造を対象に事業開発ガイド「10の視点」を策定。

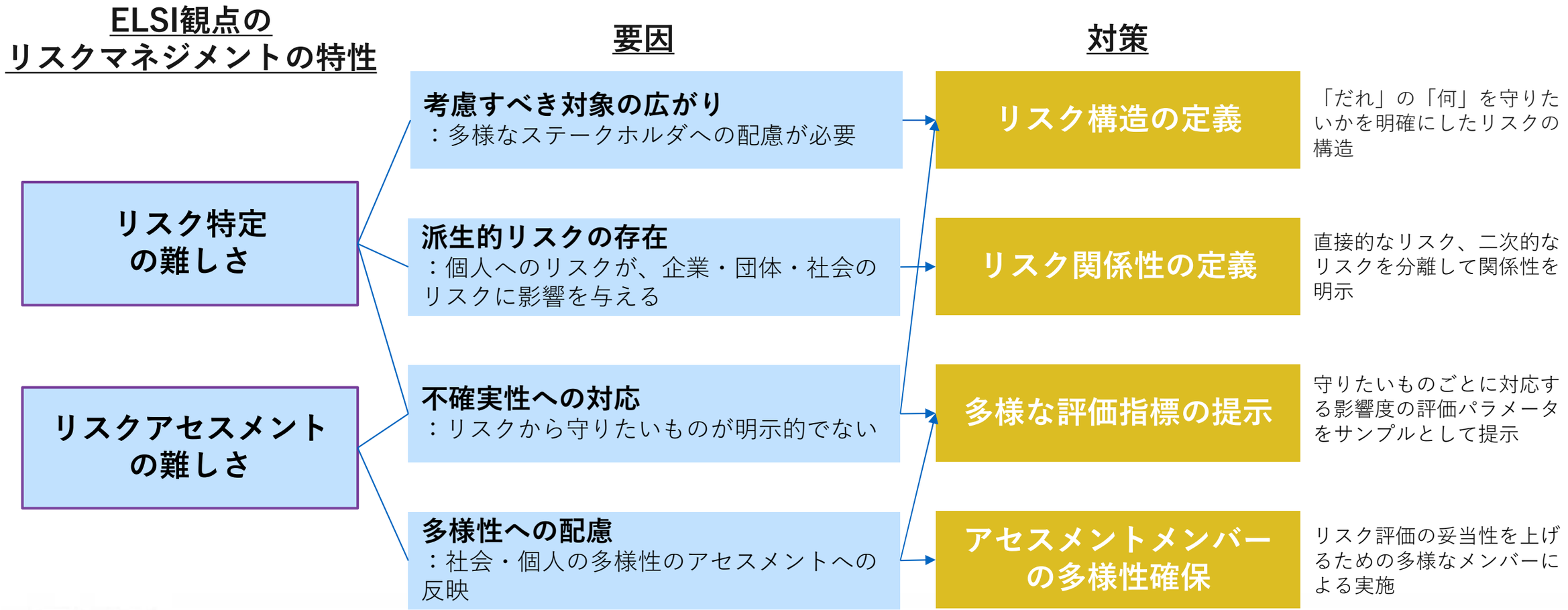
＜顔認証技術の適正利用に向けた10の視点＞

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。
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。

対象とする顔認証技術を適用した事業の構造

1．リスクアセスメント手法の特徴

難易度の高いELSI観点のリスクマネジメントを適切に行う対策を実装。



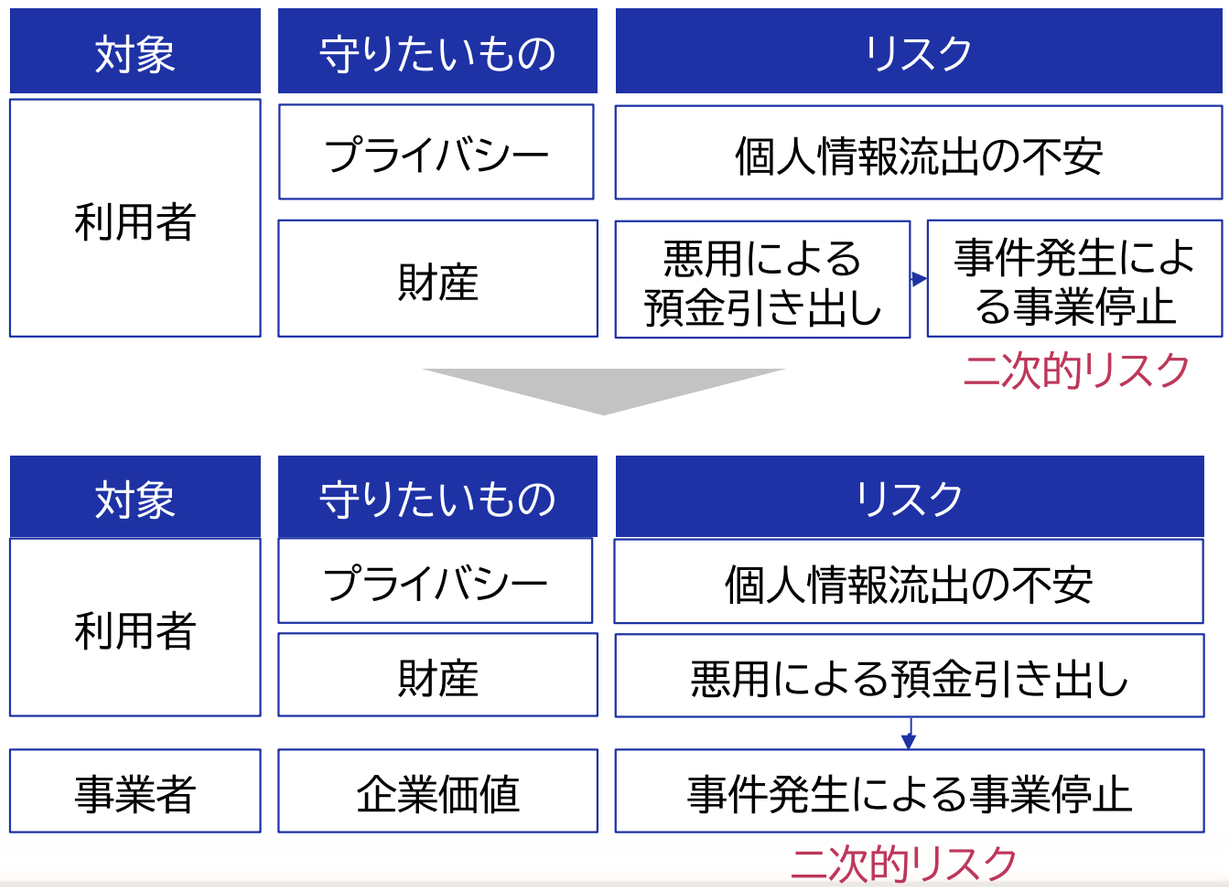
1．リスクアセスメント手法の特徴：リスク特定

リスクから守りたい“対象＝ステークホルダー” と “守りたいもの” を明示した上で、リスクの特定を行う。個人に対する直接的なリスクと、派生的に発生する二次的リスクの特定を行う。

【リスク特定の構造】

- 対象
  - リスクから守りたい対象。ステークホルダーから選定
- 守りたいもの
  - リスクから守りたいもの：財産,人権、尊厳、自由…
- リスク：直接
  - 対象・守りたいもの を毀損する可能性のある事象
- リスク：二次的
  - 派生して、二次的に発生する可能性のあるリスク

    例：利用者の財産を毀損するリスクから派生する
    事業者の企業価値を毀損するリスク

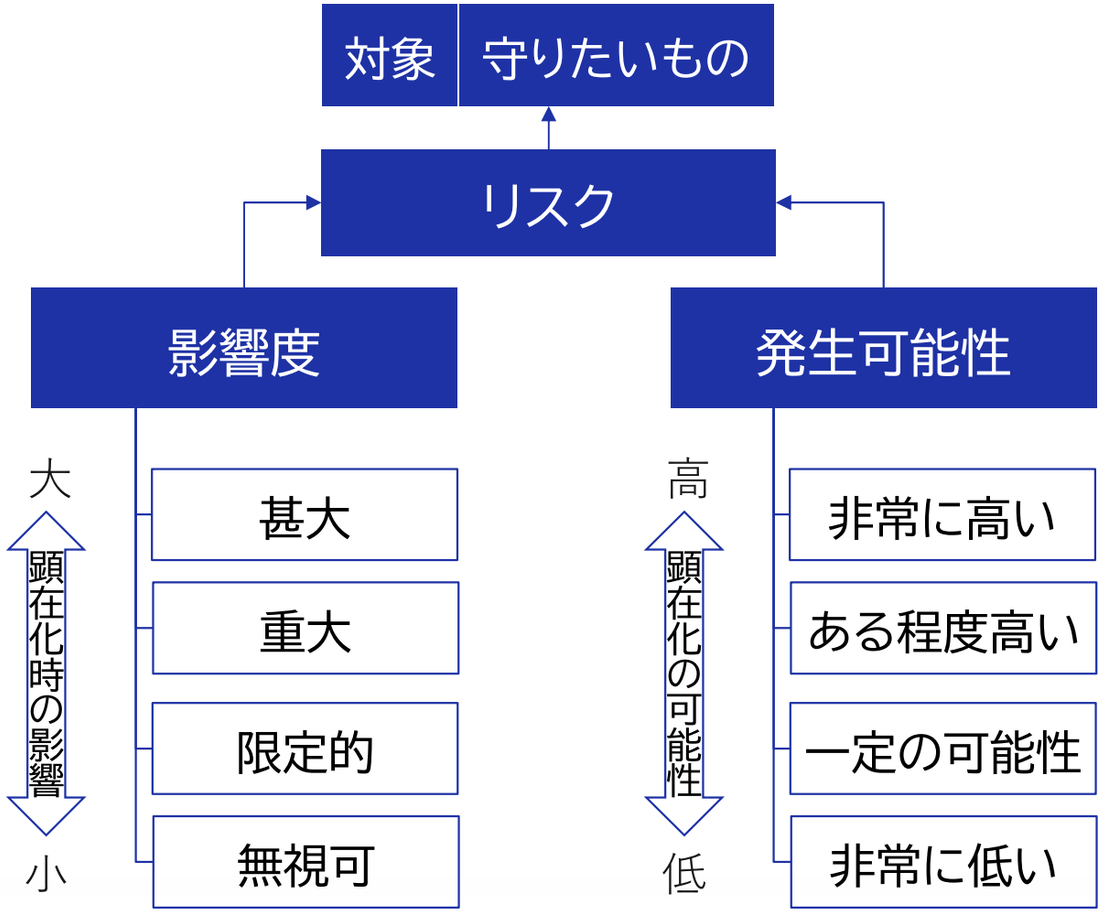


1．リスクアセスメント手法の特徴：リスクアセスメント

対象-守りたいもの毎に定義されたリスク評価パラメータサンプルを参考に、評価パラメータと閾値の設定を行い、リスク評価を行う。リスク評価は、直接リスク、二次的リスク両方に対して行う。

【リスクアセスメントの構造】

- 対象
  - リスクから守りたい対象。ステークホルダーから選定
- 守りたいもの
  - リスクから守りたいもの：財産,人権、尊厳、自由…
- リスク
  - 対象・守りたいもの　を毀損する可能性のある事象
- 影響度評価
  - リスクが顕在化した時の影響度を4段階で評価
- 発生可能性評価
  - リスク顕在化の可能性を4段階で評価



1．リスクアセスメント手法の特徴：リスクアセスメント

対象-守りたいもの毎に定義されたリスク評価パラメータサンプルを参考に、評価パラメータと閾値の設定を行い、リスク評価を行う。リスク評価は、直接リスク、二次的リスク両方に対して行う。

特定されたリスク

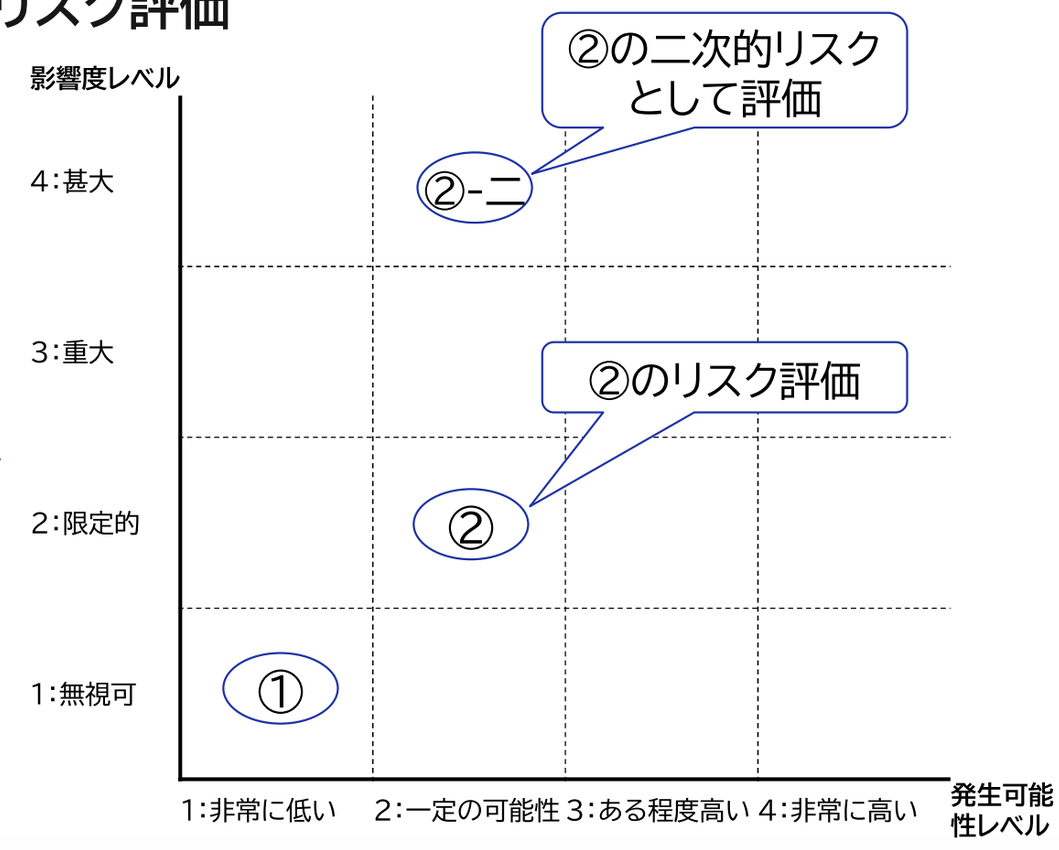
対象	守りたいもの	リスク	
利用者	プライバシー	個人情報流出の不安	①直接
	財産	悪用による預金引き出し	②直接
事業者	企業価値	事件発生による事業停止	②二次的

リスク評価パラメータサンプル

対象	守りたいもの	影響度パラメータ	パラメータの説明	甚大	重大	限定的	無視可
利用者	人権、プライバシー	社会・精神的苦痛	健康被害の重症度（死亡/重症/軽傷） 治療の負担度合い（金額/期間/等）	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
	健康	身体的影響					
	財産	経済的影響					
	尊厳	実存・精神的苦痛					
	自由	行動範囲の度合い、意思決定への影響					
	時間、機会	機会損失の程度					
	利便性、期待	がっかり、期待外れ					
	対人関係	交友関係への影響					

影響度の評価パラメータを
ELSI観点により複数設定することで
多義性含むリスクにも対応

リスク評価



2．大阪大学の顔認証入場システム

2024年6月から顔認証入場システムを試行導入。大阪大学キャンパス内の建物入口および会議室を対象に、顔認証カメラを計27ヶ所に設置。

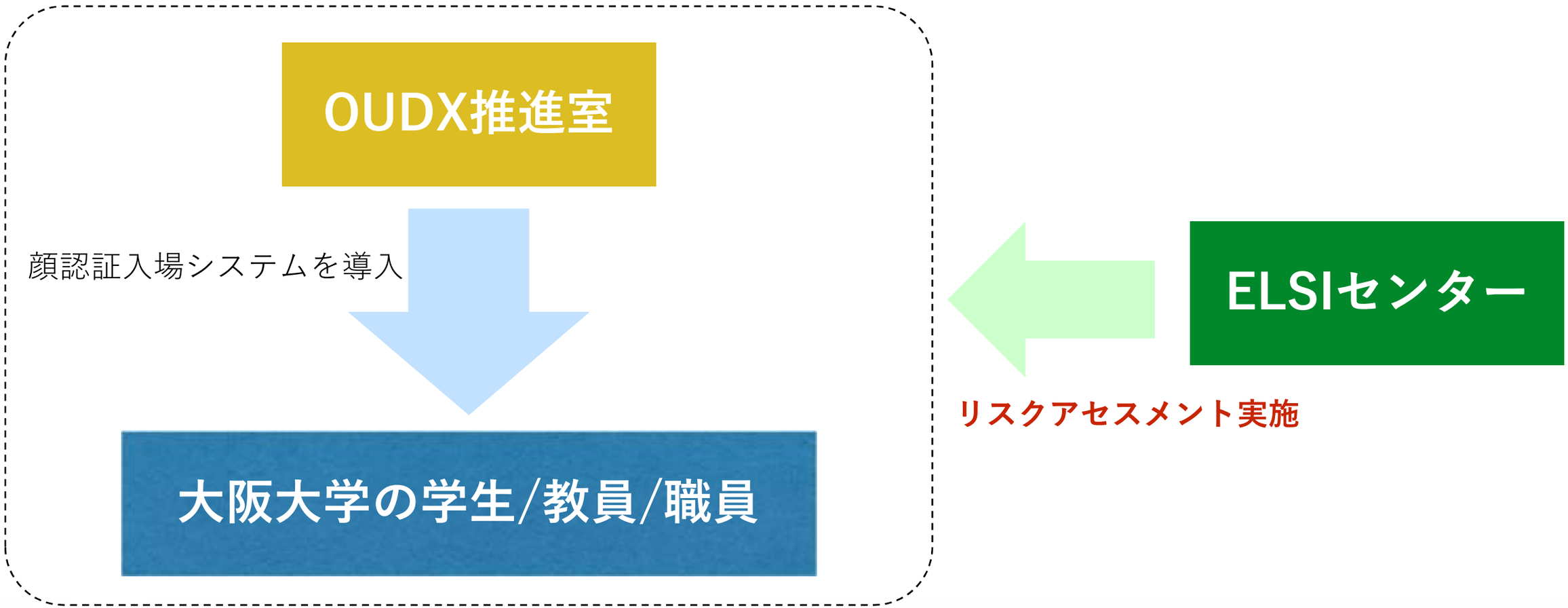
- 導入の背景
  - 建物や部屋ごとにシリンダーキーやIC・磁気カードなど、入場管理の方法が異なっていたことに加え、紛失ケース・磁気喪失ケースの多さや、手書きの鍵貸出台帳の準備や記入といった煩雑な手続きが大きな事務負担となっている。

- 顔認証入場システム
  - 大阪大学のDX推進施策の一環として顔認証入場システムの導入を計画。
  - 顔認証入場システムの利用は任意で、従来のカードキーも利用可能。
  - 利用者は専用ウェブサイト上で、プライバシーポリシーへの同意および顔写真の登録が必要。
  - 利用時は顔認証カメラに顔を向けることでドアが解錠。

建物入口に設置された顔認証カメラ

3．リスクアセスメント：概要

OUDX推進室からの依頼を受け、ELSIセンターが第三者の立場で、顔認証入場システムが試行導入される27ヶ所を対象にリスクアセスメントを実施。



3．リスクアセスメント：実施プロセス

以下のリスクマネジメントのプロセスに沿ったアセスメントを実施。共同研究成果のリスクアセスメント手法を活用。

プロセス

リスク特定	対策前のリスクアセスメント	リスク対策オプション	対策後のリスクアセスメントと残余リスク	実施後のリスクアセスメント（事後評価）
・対象ユースケースのステークホルダーを特定する。 ・「守りたいもの」を列挙し、リスクの指標を定める。 ・特定ステークホルダーに影響するリスクを洗い出す。 ・類似のリスクは１つにまとめるなどして、リスク項目を整理する。	準備） ・洗い出したリスク項目を参考に「守りたいもの」を追加/削除。 ・4段階の影響度パラメータ/レベルを設定。 ・4段階の発生可能性パラメータ/レベルを設定。 実施） ・リスク項目ごとに影響度/発生可能性を評価。	・リスクアセスメント結果に基づき、リスク項目ごとの対応方針を「回避」「低減」「保有」から選択。 ・リスク項目ごとに具体的な対策オプションを挙げ、最適な対策案を選択する。 ・その際には、技術的な実行可能性、対策費用などの利用可能なリソースなどを考慮する。	・対策実施後を想定し、リスク項目ごとの影響度/発生可能性を評価する。 ・リスク項目ごとに、残余リスクが受け入れ可能なレベルにあることを確認する。 ・残余リスクが高い項目がある場合は今後の対策の見込みを確認する。	・プロジェクトの実施後には、事後評価を実施する。 ・想定外のリスクが生じていないかどうか確認する。見いだされた場合は、リスクアセスメントを実施し、リスク対応方針を決め、対策オプションを挙げ、対策案を選択する。
アウトプット				
・ステークホルダーリスト ・リスク項目リスト	**・対策前のリスクアセスメント結果**	**・リスク対策案の決定**	**・対策後のリスクアセスメント結果**	**・実施後のリスクアセスメント結果**

3．リスクアセスメント：ステークホルダー分析

ステークホルダー分析として、大阪大学に出入りする関係者の属性を洗い出した。
キャンパス内には病院と保育園もあり、様々な関係者が存在する。

対象となる顔認証入場システムの主な利用者

学内関係者

- 学生
- 教員
- 職員
- 園児とその保護者
- 食堂や売店の従業員
- システム管理者（OUDX推進室）
- 部局ごとのシステム管理者

学外関係者

- 訪問者（他の大学、企業、行政等）
- 業者（維持管理、清掃、配達、営業等）
- 他国からの訪問者
- 周辺住民
- 病院患者
- 患者の関係者（家族等）
- 受験生

3．リスクアセスメント：リスク特定

「10の視点」を活用して計58件のリスクを洗い出し。類似リスクをまとめ、13件のリスク項目に整理。

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不安 - 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不安 - 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不安
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	**アカウンタビリティの課題**	6	サービスのライフサイクル（導入、変更、終了）を通した正当性の不足 - 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への説明不足 - 視覚障碍者への配慮不足 - 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 - 利用推進する職場での同調圧力

3．リスクアセスメント：リスク対応方針の考え方

リスクアセスメントの準備として、リスクに対する対応方針＝回避／低減／保有の考え方を定義。次工程の評価パラメータのレベル設定へのインプットにも活用。

【リスク対応方針の考え方】

- リスク項目ごとに影響度レベルと発生可能性レベルで４段階に数値化して掛け算で算定

  （リスク点数）＝（影響度レベル）×（発生可能性レベル）

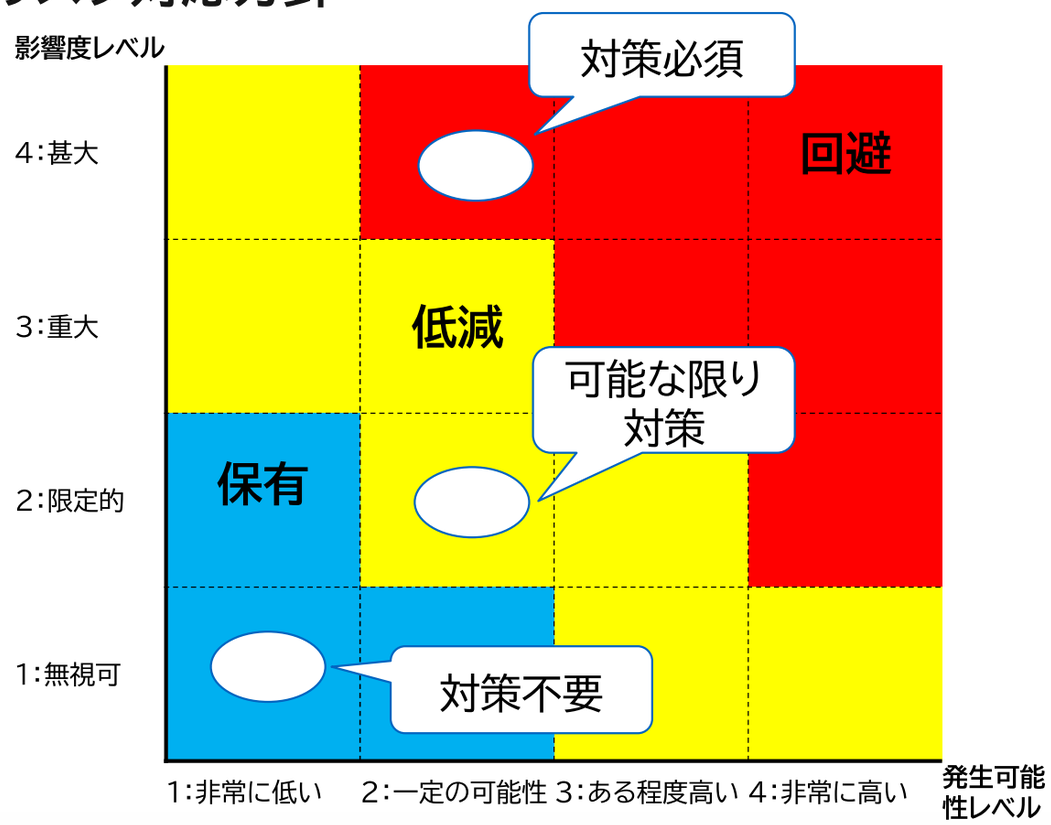
- リスク点数によるリスク対処方針を定義

  7以上：リスク回避　　⇒回避に向け対策必須

  3～6 ：リスク低減　　⇒低減に向け可能な限り対策

  2以下：リスク保有　　⇒対策不要

リスク対応方針



3．リスクアセスメント：評価パラメータとレベル設定

リスクが影響を及ぼす「守りたいもの」に対し、影響度と発生可能性で評価するための評価パラメータとレベルごとの設定を、参加メンバーで協議して定義。

評価パラメータとレベル設定の例

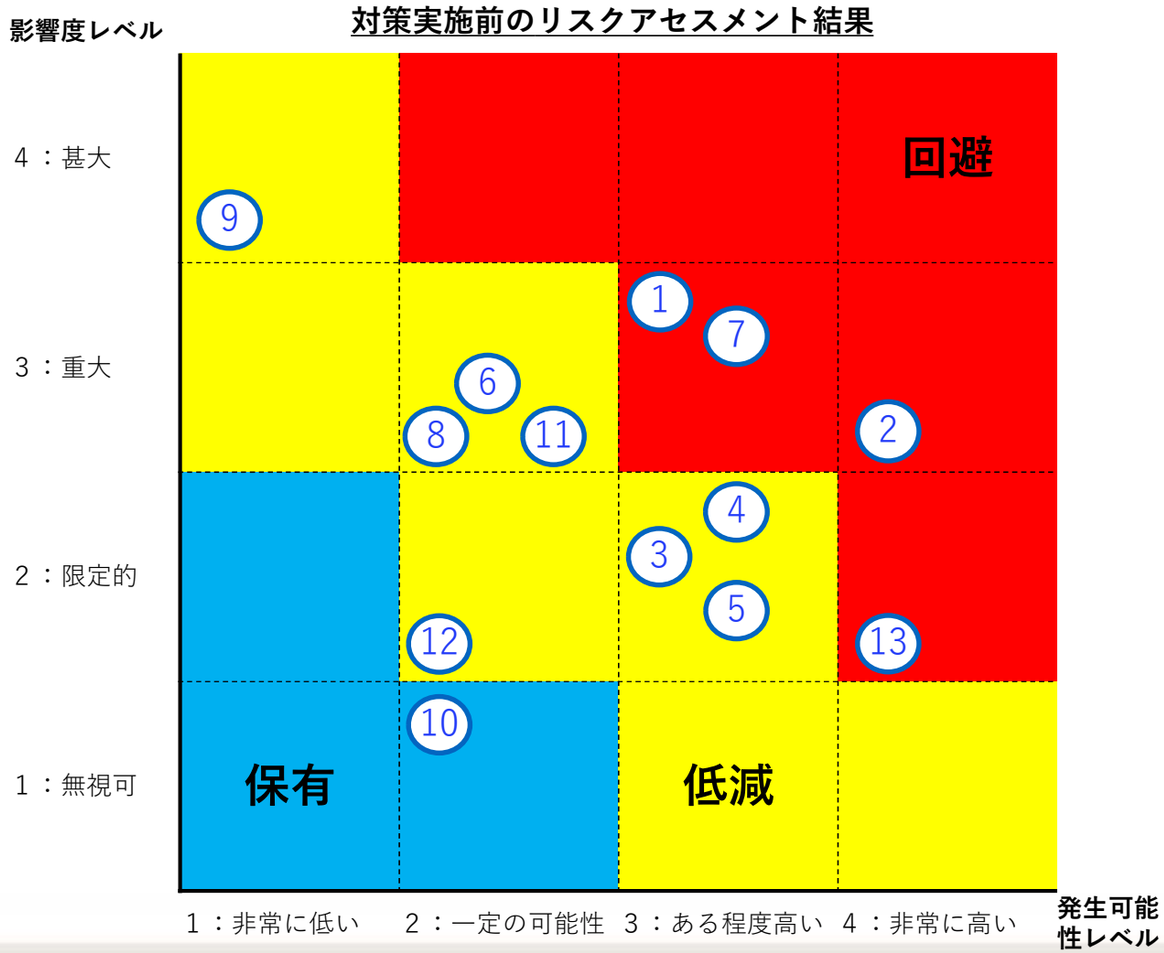
守りたいもの	評価軸	評価パラメータ	レベル４	レベル３	レベル２	レベル１
人権・プライバシー	影響度	精神的な苦痛	甚大	重大	限定的	無視可
			回復不可能なダメージ	治療が必要なダメージ	一次的なダメージ	軽微な不快感
	発生可能性	人数比率	非常に高い	ある程度高い	一定の可能性	非常に低い
			50%以上	10%以上	1%以上	1%未満

・
・
・

3．リスクアセスメント：対策実施前のリスクアセスメント結果

従来のカードキーによる入場を継続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。

No.	リスク項目
1	データの過剰収集・保存
2	プロセス面のコミュニケーションの課題
3	内容面のコミュニケーションの課題
4	公的機関への情報連携に関する不安
5	ユーザビリティの課題
6	アカウンタビリティの課題
7	誤認証
8	包摂性の課題
9	なりすまし
10	迷惑行為
11	事後検証の欠落
12	写り込み
13	有効でない同意



3．リスクアセスメント：リスク対策オプション

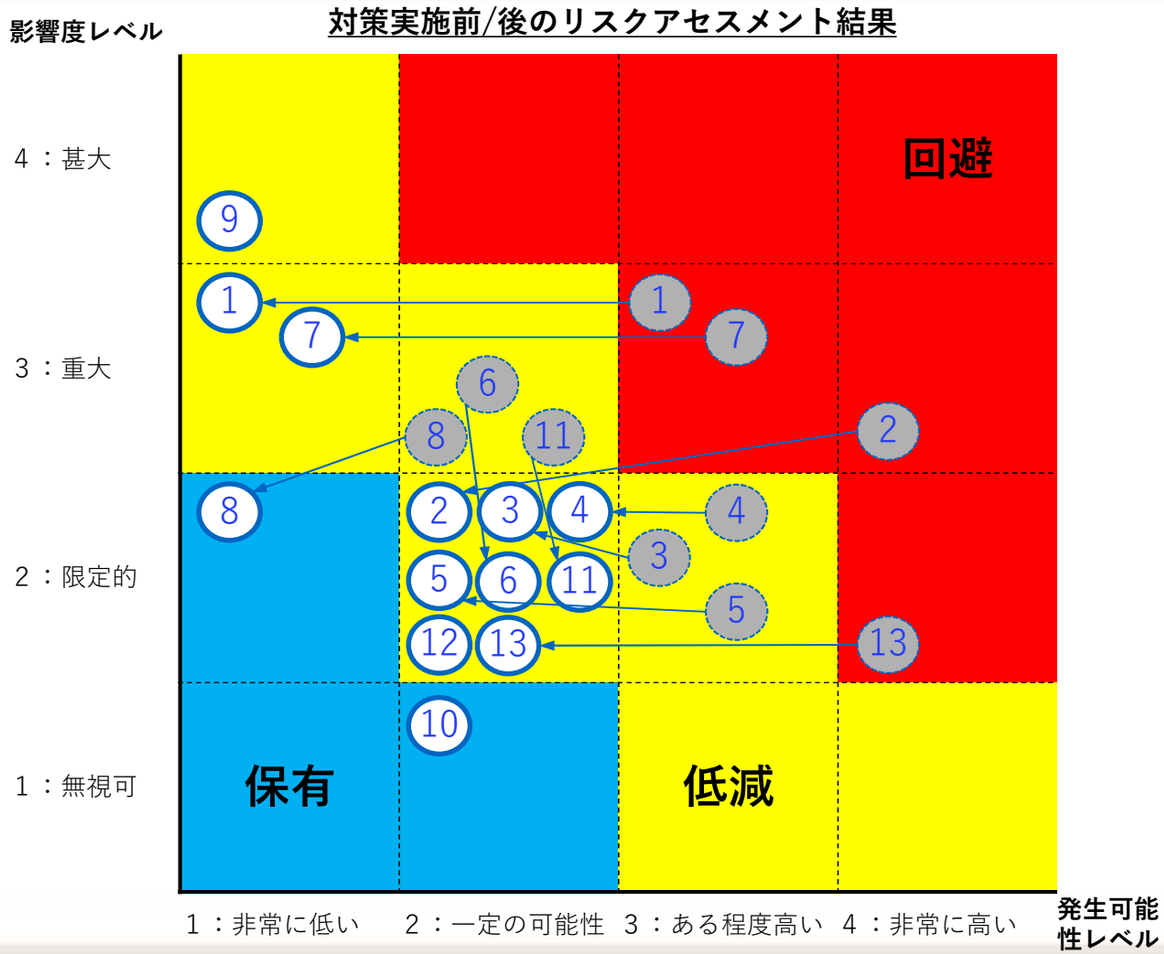
OUDX推進室に実施済みの対策をヒアリングした上で、リスク項目ごとに追加すべき対策案を参加メンバーで検討。

No.	対策案	内容	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

3．リスクアセスメント：対策実施後のリスクアセスメント結果

必要な対策を講じることでリスクを許容可能な範囲内に抑えることが可能で、対策後の顔認証入場システムの導入は大学として受け入れられるものであると結論。

No.	リスク項目
1	データの過剰収集・保存
2	プロセス面のコミュニケーションの課題
3	内容面のコミュニケーションの課題
4	公的機関への情報連携に関する不安
5	ユーザビリティの課題
6	アカウンタビリティの課題
7	誤認証
8	包摂性の課題
9	なりすまし
10	迷惑行為
11	事後検証の欠落
12	写り込み
13	有効でない同意



まとめ

- 背景
  - 大阪大学/NECの共同研究で顔認証技術の「10の視点」「リスクアセスメント手法」を策定
  - 大阪大学のDX推進施策の一環でキャンパス内に顔認証入場システムの導入を計画

- リスクアセスメント
  - ELSIセンターが第三者の立場で顔認証入場システムのリスクアセスメントを実施
  - 必要な対策を講じることで顔認証入場システムは受け入れ可能と結論

- 今後の対応
  - 利用開始後の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の実施
  - DX推進施策で導入計画している新たなサービスへのリスクアセスメントの適用

ELSI NOTE：リスクアセスメントの詳細

本リスクアセスメントの詳細はELSIセンターのウェブサイト上の「ELSI NOTE」にて公開中。


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

ELSI NOTE No.43

2024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

Authors

大阪大学


ELSI NOTE　大阪大学 社会技術共創研究センター

目次

<https://elsi.osaka-u.ac.jp/research/2922>