

顔認証を利用した顔パス イベント入場に関する

個人情報リスク評価 DPIA・PIA (Data Protection/Privacy Impact Assessment)

初版 2021年3月

弁護士 水町雅子

作成協力者 日本電気株式会社デジタル・ガバメント推進本部部長 岩田 孝一

このPIAに用いた「顔認証を利用した顔パス イベント入場プロジェクト」は、
個人情報保護に関する民間の自主的取組に資するために、
実案件を模して定義した「ダミープロジェクト」であり、
実在の人物・団体・事件などには一切関係ありません。

Agenda

- 1 顔パス入場とは
 - 1.1 顔パス入場の概要
 - 1.2 顔パス入場の仕組み
- 2 本評価について
 - 2.1 本評価の目的
 - 2.2 本評価の対象
 - 2.3 顔パス入場全体図と本評価の対象詳細
- 3 顔パス入場の個人情報保護のポイント（対策まとめ）
- 4 顔パス入場全体スキーム・関係者図
- 5 リスク対策
 - 5.1 なりすまして別人が入場することはないのか
 - 5.2 誤認証・誤認識で入場できないことはないのか
 - 5.3 入場するために顔画像を登録しなければならないのか
 - 5.4 顔画像や特徴量等の個人情報は誰がどこで保管するのか
 - 5.5 顔認証・顔画像が不正利用されないのか
 - 5.6 漏えい対策は
 - 5.7 もし特徴量が漏えいしたらどうなるのか
 - 5.8 知らない間に顔画像が撮影されないのか
 - 5.9 顔画像や特徴量を他人に提供することはないのか
 - 5.10 顔写真・特徴量を確実に削除するのか
 - 5.11 監視につながらないのか
 - 5.12 その他のリスク対策（個人情報の取得に関して）
 - 5.13 その他のリスク対策（個人情報の利用・提供に関して）
 - 5.14 その他のリスク対策（個人情報の安全管理措置に関して）
 - 5.15 その他のリスク対策（個人情報の管理に関して）
 - 5.16 その他のリスク対策（全般に関して）
 - 5.17 個人情報保護法への適合性（抜粋）
- 6 総括
 - 6.1 まとめ
 - 6.2 水町雅子のコメント
- 7 参考
 - 7.1 パーソナルリファレンスアーキテクチャ
 - 7.2 本評価書と特定個人情報保護評価書との対照関係
 - 7.3 参考URL

1 顔パス入場とは

1.1 顔パス入場の概要

①申込時



利用者

- ・ Webから申込み
- ・ 氏名、生年月日、住所、電話番号、メールアドレス、パスワードを入力する
- ・ 「顔パス入場」を利用したい場合に限り、顔写真データの登録の同意を行い、顔写真データをアップロードする
- ・ いったん登録した後に、顔写真登録の取消も可能

②入場時



顔パス利用者

※顔パス入場者以外は、通常ゲートから通常通り入場

- ・ 顔パス入場者は、顔パス入場ゲートのカメラで撮影した顔写真データをアップロードして識別・認証することの同意を行う。同意された場合のみウォークスルー用のゲートに進む
- ・ ゲートのカメラで顔写真を撮影
- ・ 認証できた場合は、入場ゲートが自動的に開く
- ・ 認証できなかった場合は、通常ゲートから通常通り入場するか、係員に問い合わせる

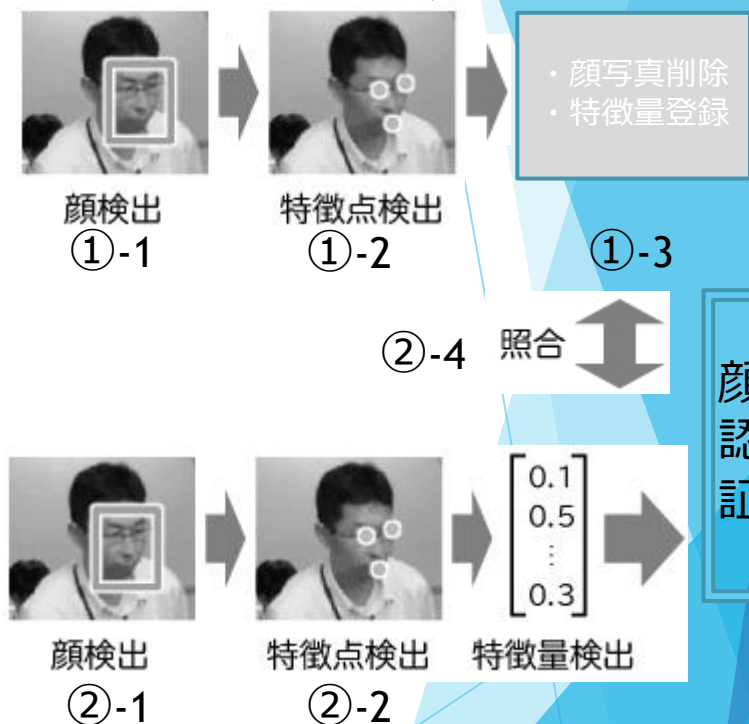
1.2 顔パス入場の仕組み

①申込時

- ①-1 利用者が登録した画像中から顔を検出
- ①-2 顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した特徴量を抽出
- ①-3 利用者が登録した顔写真データを削除、特徴量をイベント管理システムに登録

②入場時

- ②-1 顔パス入場ゲートのカメラで撮影された画像中から顔を検出
- ②-2 顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した特徴量を抽出
- ②-3 撮影された顔写真データを削除
- ②-4 ゲートのカメラで撮影された画像の特徴量データ（②-2）と、利用者が登録した画像の特徴量データ（①-2）とで顔識別・顔認証を実施し、認証できた場合はゲートを開放
- ②-5 ゲートのカメラで撮影された画像の特徴量データ（②-2）を削除



2 本評価について

2.1 本評価の目的

顔認証のメリットと懸念

- 顔認証により、来場者は手ぶら（チケットレス）で、そして入場待ち時間が短縮する等、スムーズにイベントに参加することができます。また、不正入場の防止や接触レスなどの利点もあります。他方で、重要な個人情報である顔画像が万一悪用されたり流出してしまえば、プライバシーに与える影響は非常に大きく、また様々な場所での監視につながる懸念や、顔認証の精度の問題等もあります。

個人情報やプライバシー権の保護が大前提

- 顔認証の活用といった比較的新しい取組みはイノベーションに欠かせないものではありませんが、個人情報やプライバシー権の保護がまずもって大前提であり、プライバシーに与える悪影響を防止・軽減する対策を事前に十分講じた上で、適法・適正に技術が活用されていくことが重要です。

顔認証に対するプライバシー影響評価

- 個人情報・プライバシー権保護のための手法として、海外で普及する「DPIA*」「PIA**」というスキームがあります。ビジネスを開始する前に、そのビジネスが個人情報・プライバシーに対してどのような悪影響を与える可能性があり、その悪影響を防止・軽減するためにどのような対策を講じるかを検討するスキームです。
- 本評価では、「DPIA」「PIA」スキーム（以下、単に「PIA」といいます。）を用いて、顔認証を利用したイベント入場におけるプライバシーへの影響及びそれを防止等する措置を検討します。

*DPIA：GDPR（一般データ保護規則）に規定されたデータ保護影響評価（Data Protection Impact Assessment）

**PIA：英・米・カナダその他の様々な国で実施されているプライバシー影響評価（Privacy Impact Assessment）

2.2 本評価の対象

- 個人情報保護委員会「個人情報保護に関する民間の自主的取組の在り方」に関する調査の一環として、顔認証サービスを展開する日本電気株式会社（以下、「NEC」といいます。）及びJIPDEC（一般財団法人日本情報経済社会推進協会）協力の下、顔認証を利用したイベント入場に関して DPIA・PIA スキームを用いた本評価を実施しました。
- 本評価は、弁護士水町雅子が、NECから資料提供やヒアリングを受けながら実施し、上記個人情報保護委員会「PIA検討会」に提出したものです。なお、NECは、本評価書に記載された内容に偽りがないことを事前に確認しています。
- 本評価は、「NEC顔認証機能を利用した顔パスイベント入場」（以下「顔パス入場」といいます。）をその範囲・対象としています。NECは様々な場面（出入国管理、企業の入退室管理、顔認証決済等）で利用できる顔認証サービスを提供していますが、今回は顔認証を利用したイベント入場を対象に、本評価を実施します。なお、顔認証入場に際する個人情報・プライバシー保護全般を目的としており、実際に稼働しているイベント入場に対する評価ではなく、NEC顔認証技術を元にイベント入場管理を行うことを想定した評価になります。そのため、本評価中に登場するX社・Y社はあくまで仮定の企業になります。

3 顔パス入場の個人情報保護のポイント（対策まとめ）

顔写真データは、大変重要な個人情報です。また、顔認証が悪用等されると、なりすましや監視等につながる懸念もあります。顔認証技術を利用・提供する企業にはこれらのリスクその他のプライバシー権侵害や不正行為を防止するため、様々な対策を応じる必要があります。NECでは本評価記載の通りの措置を講じており、その主なポイントは以下の通りです。

主なポイント

① 顔写真データ自体はすぐに削除

- ・ 顔写真データを利用者が登録後、速やかに顔認証システムでは「特徴量抽出*」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。
- ・ 来場時にゲートで撮影した顔写真データも、速やかに特徴量抽出を行い、撮影データを削除します。

*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

② 希望者だけが、顔パス入場

- ・ 顔パス入場希望者以外は、通常ゲートから通常通り入場できます。

③ NECが提供する顔認証機能では、氏名・住所等の情報は保持しません

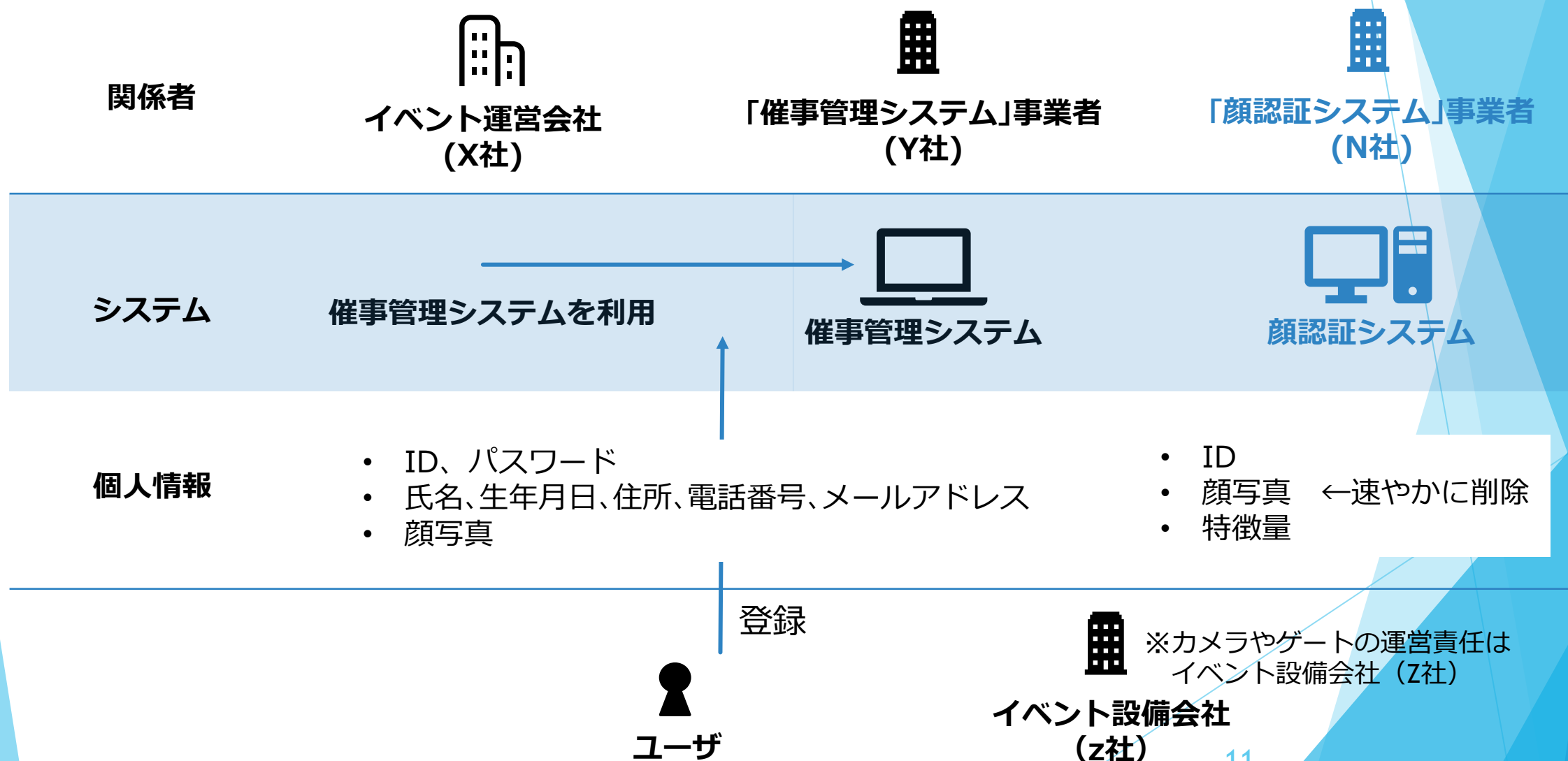
- ・ ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
- ・ 但し、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しています。

④ セキュリティ

- ・ 様々なセキュリティ対策を履践しています。NECではPマーク付与認定及びISMS認証を取得しています。

4 顔パス入場全体スキーム・関係者図

※本評価はN社のリスク対策を主としており、実際に稼働しているイベント入場に対する評価ではないため、X・Y社で行うべきリスク対策等が残存リスクとして残ります。



5 リスク対策

個人情報・プライバシーへの影響とその対策

5.1 なりすまして別人が入場することはないのか



激戦を勝ち抜いてチケットを獲得しました。

別人が私になりすまして勝手に入場し、私が入場できなくなることはないのでしょうか。

高精度の認証技術

- 骨格の似た親兄弟でも違いを検知し、双子についても違いを判別します。
- NECの生体認証は、約70の国と地域1000システム以上の導入実績があります。なかでも顔認証は入出国管理や国民IDなど国家レベルでのセキュリティのほか、企業での入退管理や端末ログイン、決済など、様々な用途で使われています。
- NECの顔認証技術は、米国国立標準技術研究所（NIST）主催のベンチマークでNo.1の評価を5回獲得しています。米国国立標準技術研究所(NIST)が実施した最新の顔認証技術のベンチマークテスト(FRVT2018)において、1,200万人分の静止画の認証エラー率0.5%という、第1位の性能評価を獲得しました。なお、NISTのベンチマークテストは数千万人規模の大規模静止画データにおける認証精度と処理速度を評価するもので、使われる評価画像は、登録用画像として1200万人分の静止画像が登録され、照合画像としては未登録人物33万人分、登録人物15万人分が利用されるというものです。

<https://jpn.nec.com/biometrics/face/index.html>

- 今後も、精度の維持・向上に努めていくことが求められます。

不正対策も

- 顔認証システムでは、「いつ・だれが入退したか」というデータをログとして正確に残せます。そのため、万一不正が起こっても、究明が可能です。
- 万一不正が起こった場合は、通常ゲートの会場係員が、催事管理システムからお客様のチケット情報を確認したり、どのような人物がお客様のチケットを用いて入場したかどうかを確認します。

5.2 誤認証・誤認識で入場できないことはないのか



激戦を勝ち抜いてチケットを獲得しました。
それなのに、顔認証システムが私を認識してくれなくて、入場できなくなることはないのでしょうか。

マスクやサングラス、横向きでも認証が可能

- NECの顔認証は、マスクやサングラスなどを装着した場合でも、事前に登録した画像データと照合し、本人かどうかを高精度で識別できます。人工知能（AI）の手法の一つである深層学習に、本人と似ている他人との違いを強調する独自の工夫を取り入れ、精度を高めることができました。マスクやサングラスを装着していたり、顔を横に向けていたりしても、正面で撮影した画像をもとに高精度で認証することができます。

入場前であれば顔写真データの差替も可能

- 昔の顔写真で申し込んでしまった場合や、申込後に顔を負傷した場合等であっても、入場前であれば、申込ページにログインいただいたうえで、顔写真データを差し替えることができます。

通常ゲートから入場可能

- 万一、認証エラーになった場合は、通常ゲートから通常の方法で入場できます。
- お客様が当日チケットをお持ちでなかったとしても、Web画面からお客様自身で催事管理システムにログインし、ご自身のチケット情報をご確認いただけますし、会場係員も催事管理システムにログインし、確認することができます。

5.3 入場するために顔画像を登録しなければならないのか



某イベントに参加したいです。
でも、そのために顔画像を登録したり顔認証をするのは嫌です。

希望者だけ、顔画像による顔パス。通常ゲートからチケット提示でも入場できます

- 顔認証による顔パス入場は、あくまで希望者だけが対象。
- 顔パス入場以外に、通常ゲートからチケットを提示し、通常の方法で入場することができます。顔パス入場か通常入場かは自由に選択可能です。通常入場を選択した場合にも来場者に不利益はありません（もっとも、通常入場の際は、入場待ちリスク、係員との接触リスク等はある）

取消可能

- 一度顔パス入場を申し込んだ方でも、顔パス入場する前までであれば取消が可能。
- 取消を希望された場合は、顔写真、特徴量その他の個人情報を速やかに削除します（但し、問合せ対応のためIDだけは取消済のIDとして記録し保持しておく）。

残存リスク

- 取消時については、NECだけでなく、X社・Y社においても確実に削除されることを確認する必要があります。

5.4 顔画像や特徴量等の個人情報とは誰がどこで保管するのか



私の顔画像や特徴量、氏名などの個人情報は誰がどこで保管するのですか？

NECでは顔写真、特徴量、IDのみ保持

- NECでは、顔写真データ、顔写真データから抽出した特徴量、IDのみを保持します。このうち、顔写真データは下記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
- また、NEC顔認証機能で生成した特徴量は、X社・Y社に提供することはありません。NEC顔認証機能内で削除するまで保存されますが、X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。
- NECにおけるこれらの情報の管理方法・リスク対策については、5.6「漏えい対策は」を参照ください。

顔写真、氏名、住所等はX社・Y社

- ID・パスワード、氏名、生年月日、住所、電話番号、メールアドレス、顔写真といった、申込時に登録等していただいた情報は、イベント運営会社X社の責任で保管されます。
- 責任主体はイベント運営会社X社ですが、保管場所はイベント運営会社X社が利用する、Y社催事管理システムになります。Y社催事管理システムの提供・運営・保守等、X社から委託の範囲内でこれらの個人情報にアクセスすることができます。またX社もこれらの個人情報にアクセスすることができます。
- X社・Y社では上記の通り、特徴量はいっさい保持せず、NECから顔認証OKかNGかの情報が提供されるだけです。
- 4「顔パス入場全体スキーム・関係者図」もあわせてご覧ください。

残存リスク

- 催事管理システムでの管理方法・リスク対策については、催事管理システム事業者Yに確認する必要があります。
- ゲートカメラのデータ自体については、イベント設備会社Z社に確認する必要があります。

5.5 顔認証・顔画像が不正利用されないのか



顔画像を不正コピー等されて、違う目的に利用されることはないのですか？

顔パス入場にのみ利用します

- 顔認証・顔画像は、顔パス入場にのみ利用します。
- NECは委託を受けて顔認証機能を提供する立場であり、登録された顔画像とゲートで撮影された顔画像が一致するか否かを判断する目的以外に個人情報を利用することは、リーガルのにもできません。NECでは顔画像・特徴量の不正を防止するため、社内で権限を与えられた者以外はアクセスできないよう制御し（アクセス制御、入退館・入退室制限等）、アクセス者には守秘義務を課しています。また、顔画像・特徴量を保持する顔認証システムでは逐一ログを取得し、不正コピー・不正持出し・不正提供等を監視します。
- なお、特徴量はNECでのみ保持し、委託業務終了後に廃棄します。

残存リスク

- イベント運営会社X社がどのように個人情報を利用・管理するかどうかは、X社が通知・公表等する利用目的を確認する必要があります。
- 催事管理システム事業者Y社は、一般にX社から委託を受けて催事管理システムで入場申込・入場管理等の機能を提供する立場であり、委託の範囲を超えて個人情報を利用することはリーガルのにもできません。但し、Y社における個人情報の管理方法は、Y社に確認する必要があります。

5.6 漏えい対策は



顔画像や特徴量が漏えいしたら大変ではないですか？

対策

- NECでは、クラウドサービス等を行う上で重要とされるISO/IEC20000(JIS Q 20000:2007)、ISO9001(JISQ9001)、ISO/IEC27017、ISO/IEC27018、ISMS(ISO/IEC 27001/ JIS Q 27001)、プライバシーマーク(JIS Q 15001)、SOC1/SOC2、事業継続マネジメントシステム(ISO/IEC22301)等の認定・認証を取得しています。
- 開発プロセスの各フェーズで、セキュリティの観点から実施すべき事項をセキュリティタスクとして定義し、それらのタスクをガイドラインに沿って実行することで配備されるソフトウェアは、適切なソースコード診断、脆弱性診断を経て実装されます。
- 不正プログラムの混入やその攻撃による各種の脅威（情報漏洩や可用性低下など）に対抗するために、ウイルス対策ソフトの導入、安全なプログラム設定、不要プロセスの削除等をセキュリティポリシーに纏め、同ポリシーに準拠した設計・構築及び運用体制を確立しています。
- 物理サーバのハードウェア障害時には別物理サーバにて仮想サーバの自動再起動を行うなど、ハードウェアの故障等によるサービス停止リスクに対抗するための各種設計に基づいて、構成・運用をしています。
- システムの事故（ハードウェア 障害など）に対しては、適切なモニタリングを行うことでそれを検出し、可及的速やかに障害からの復旧を行います。
- 広域災害などサービスを継続できなくなる事態に備えて、遠隔地に退避したアプリケーションとデータを復旧することのできる環境で提供しています。
- インターネットに接している IPアドレスに関しては、脆弱性を定期的にスキャンしています。

5.6 漏えい対策は



顔画像や特徴量が漏えいしたら大変ではないですか？

対策

- 故障等によりストレージデバイスを交換する場合には、データ流出を防止するための廃棄プロセスが定義されており、それに従った廃棄（NSA（米国家安全保障局）推奨方式や DoD（米国防総省）準拠方式等の消去方式）を徹底しています。
- 盗聴による影響を軽減するために専用線接続サービスやVPN（公衆網内に構成するプライベートネットワーク）を採用し、さらにIDS（不正侵入検知システム）を利用することで不審なアクセスの試みを検知しています。
- システムメモリ上、またはハードウェア上に何らかの原因で残存するデータの処理に関して適切な管理を行うために、論理的なデータの取り扱い、物理的なデータが記録されている媒体の取り扱いに関して適切な運用規定を設け、運用管理を徹底し、運用内容は第三者機関によって定期的に監査され、必要に応じて改善を実施しています。
- ID アクセス管理機能で、リソースへのアクセスを安全にコントロールすることができ、運用担当者の特権 IDの利用に対して有効な統制を実施し、組織内で要求されるアクセス制御を確実に実施しています。

残存リスク

- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社がどのように個人情報管理するかどうかは、それぞれの事業者を確認する必要があります。

5.7 もし特徴量が漏えいしたらどうなるのか



NECでは、顔写真データはすぐ削除し、特徴量とIDのみ保持するということはわかりました。IDと特徴量が漏えいした場合、特徴量から私の顔がわかるのですか？
また漏えいした特徴量を悪用して、不正ななりすましが起きませんか？

特徴量から顔画像の復元は困難です

- 現在の技術では、特徴量データから、顔画像データを復元することは困難です。特徴量データは、顔画像データ（元の生体情報）から不可逆的な方式で変換しています。また特徴量は顔の一部分の特徴のみ抽出するため、特徴量では把握できていない顔の部分が存在します。
- 特徴量データは、日本の個人情報保護法では「個人識別符号」に該当する情報です。氏名や顔画像データなどと紐づけて管理されていなくても、特徴量データ単体で個人識別符号に該当し、明確に個人情報であると定義されています。個人情報保護法に従って、NECでは厳格な管理を実施しています。
- 生体情報は、パスワードなどと異なり、他人に盗み見られたり、わすれてしまうリスクがありません。他方で、その人しか持たず簡単に変更できないという生体情報のメリットは、漏えいしてしまった場合に深刻な問題となります。「一生変わらない」という生体情報のメリットは、「一生変えられない」というデメリットにもなり得ます。そのため、生体認証技術を使う際の生体情報の管理には、厳重なセキュリティ対策が求められます。

5.8 知らない間に顔画像が撮影されないのか



知らない間に顔画像を撮影したり、顔認証したりしないですか？

知らない間に顔認証することはありません

- **顔パス入場ゲートでのみ**顔認証を行います。顔パス入場ゲートは通常ゲートと異なる**外観**になっており、顔認証を実施することを立看板で**周知**しています。
- なお、顔パス入場ゲートで顔画像を撮影した場合であっても、**事前に顔写真を登録していない場合は**顔認証エラーとなります。そして顔パス入場ゲートで撮影された顔画像・特徴量データは速やかに削除されます。
- 顔パス入場ゲート以外では、顔認証を実施しません。

残存リスク

- ゲートカメラの運営はイベント設備会社Z社に委ねられています。ゲートカメラで常時撮影しているか、人がカメラ前に立った時だけ撮影しているのかは、Z社に確認する必要があります。

5.9 顔画像や特徴量を他人に提供することはないのか



顔画像や特徴量を他人に提供することはないですか？

第三者提供は行いません

- NECでは、個人情報保護法に反して、顔画像や特徴量を第三者提供することはありません。NECでは顔認証システムの保守運用等に関して必要な範囲内で委託を行う可能性がありますが、その場合も、個人情報保護法及び同ガイドラインに則って委託先を監督します。
- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社においても、法律に反した第三者提供を行えば、個人情報保護法違反になります。
- なお、個人情報保護法で認められている外部提供として、例えばイベント会場内で犯罪が発生した場合で、警察から令状に基づき来場者情報の提供を求められた場合等は、氏名・顔画像等を警察に提供することがあります。

残存リスク

- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社が、個人情報保護法を遵守した上で共同利用等を行う可能性も考えられなくありませんので、それぞれに確認する必要があります。

5.10 顔写真・特徴量を確実に削除するのか



顔画像や特徴量は確実に削除してもらえるのですか？
私が自分で削除依頼をしないといけないのですか？

顔写真データはすぐに削除します

- （申込時）顔パス入場を希望するユーザは顔写真データを登録します。その後、速やかに顔認証システムでは「特徴量抽出*」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。
- （来場時）ゲートで顔写真を撮影し、特徴量抽出*を行った上で、上記申込時に登録された特徴量と比較して顔認証を行います。顔認証システムでは、ゲートで撮影した顔写真データも速やかに特徴量抽出*を行い、速やかに撮影データを削除します。
顔認証の実施後は、特徴量も速やかに削除します。
- スキーム詳細は前記スライド1.2をご参照ください。
*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。
- 削除に当たって申込者の方で特に必要な手続・操作等は一切なく、顔認証システム側で**自動的に削除**します。

残存リスク

- 催事管理システム側でも顔写真データを保持するので、同システムでの削除については催事管理システム事業者Yに確認する必要があります。
- ゲートカメラのデータ自体については、イベント設備会社Z社に確認する必要があります。

5.11 監視につながらないのか



カメラで様々な情報を撮影し、様々な場所の撮影データ等とつなげれば、人の行動履歴等がつぶさにわかるのではないのでしょうか。



監視社会につながらないのでしょうか。

最小限のデータしか取得しないように措置を講じています

- **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**
 - ・ NECでは、ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
 - ・ また、NEC顔認証機能で生成した特徴量は、X社・Y社に提供することはありません。NEC顔認証機能内で削除するまで保存されますが、**X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。**
 - ・ なお、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しており、Y社は委託の範囲内でこれらの個人情報にアクセスすることができます。またX社もこれらの個人情報にアクセスすることができます。

本件顔パス入場にしか使いません

- 本件で得た顔写真データ及び特徴量は、本件顔パス入場にしか使いません。

残存リスク

- X社・Y社で、本件顔パス入場以外に利用したり、申込者が本件顔パス入場のために提供した個人情報以外と結合したりするリスクがありますので、X社・Y社に確認する必要があります。
- ゲートカメラ自体のプライバシーリスク対策については、イベント設備会社Z社に確認する必要があります。

5.12 その他のリスク対策 (個人情報の取得に関して)

上記のほか、個人情報の取得に際して次の措置を講じています。

個人情報を過剰取得しないか

- 5.11「監視につながらないのか」参照

不正確な個人情報を取得しないか

- 本人から直接顔写真データ等の提供を受けた上で、顔パス入場ゲートで実際に来場した人の顔写真を撮影して顔認証を行います。
- 本人が顔写真データ等を登録する際は、確認・修正画面から、登録内容を確認し、誤りを修正等することができます。

取得の際に個人情報が漏えい・紛失等しないか

- 本人が顔写真データ等を登録する際は、Web画面から氏名、生年月日、住所、電話番号、メールアドレス、希望パスワード等の入力・確認を行うと申込者IDが付番され、電子メールで通知されたURLにアクセスすることで登録完了します。登録完了後は、申込者IDとパスワードでWeb画面にアクセスし、登録内容の修正・削除を行うことができます。
- Web画面、「催事管理システム」、「顔認証システム」といった各間の通信は、HTTPSで通信し、通信暗号化とサーバー認証を行っています。

取得の際に不正が起きないか

- 本人の同意に基づき本人から直接顔写真データ等の登録を受ける方法を取っており、本人の知らない間にデータを取得することはありません。また、登録された顔写真データだけでは顔認証が行えず、顔パス入場ゲートで実際に来場した人の顔写真を撮影して顔認証を行います。
- また5.11「監視につながらないのか」の通り、顔パス入場の目的達成に必要な最小限の範囲内でのみ個人情報を取得します。

5.13 その他のリスク対策 (個人情報利用・提供に関して)

上記のほか、個人情報利用・提供に際して次の措置を講じています。

個人情報を無関係の者に利用されないか

- NECが提供する顔認証機能にアクセスできるのは、NECで正当な手続を経て権限を付与された社員・委託先のみです。NEC社員や委託先であっても誰でも閲覧できるわけではなく、業務上必要な範囲内で、正当な社内手続に沿ってアクセス権限を認められた範囲にのみアクセスできます。
- 5.11「監視につながらないのか」の通り、X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。

本件関係者が個人情報を私的利用・私的複製・悪用等しないか

- →5.5「顔認証・顔画像が不正利用されないのか」、5.6「漏えい対策は」参照。

個人情報が不正提供されないか

- →5.9「顔画像や特徴量を他人に提供することはないのか」参照。

目的外利用・過剰紐づけされないか

- →5.5「顔認証・顔画像が不正利用されないのか」、5.11「監視につながらないのか」参照。

5.14 その他のリスク対策 (個人情報の安全管理措置に関して)

上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- NECはJIS Q15001等に沿って個人情報保護マネジメントシステムを確立するために、「個人情報保護マネジメントシステムガイドライン」群を定めて、遵守しています。
- 事務取扱責任者を定め、各事務取扱責任者の責任範囲を規定します。事務取扱責任者は、事務取扱担当者を明確にし、各事務取扱担当者の役割と個人情報の取扱範囲を規定します。
- 事務取扱責任者は、個人情報の取扱状況を確認するために、個人情報ファイルの利用・出力状況の記録、書類・媒体等の持ち運びの記録、個人情報ファイルの削除・廃棄記録、削除・廃棄を委託した場合の確証、情報システムの利用状況の記録（ログイン実績、アクセスログ等）を記録します。
- 事務取扱責任者は、個人情報ファイルの取扱状況を確認する手段として、各個人情報ファイルの名称、種類、利用目的、取扱部署、責任者、アクセス権を有する者、削除・廃棄の方法を記録します。
- 事務取扱責任者は、管理区域において個人情報の情報漏えいを防止するために、情報システム機器等を設置するマシン室を「管理区域」として特定、入退場の履歴を記録（システムログ）、持ち込む機器を限定し、許可した機器以外の持ち込みを禁止、生体認証とその他個人認証（専用入室ICカード、社員証等）により、許可された者だけが入室できるように制限することを行います。
- 事務取扱責任者は、管理区域及び取扱区域において、個人情報記録された情報機器及び電子媒体等は、紛失又は窃盗による情報漏えい等を防止するため、情報機器、電子媒体および書類等は、キャビネットや書庫等に施錠し保管、デスクトップ端末等においてキャビネットや書庫等に施錠保管が困難な機器は、セキュリティーワイヤー等で移動や持ち出しができないよう固定することを行います。

5.14 その他のリスク対策 (個人情報の安全管理措置に関して)

上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- 事務取扱責任者は、管理区域又は取扱区域から、もしくは管理区域又は取扱区域へ、個人情報が記録された情報機器、電子媒体および書類等を持ち運ぶ際には、情報機器、電子媒体や書類等を持ち運ぶ際の記録、情報機器、電子媒体や書類等を持ち運ぶ際に、紛失や盗難等が生じないように運搬担当者が安全な処置を講ずることを確認、機器、電子媒体や書類等を持ち運ぶ際に、紛失や盗難等に備え、追跡ができるよう持ち運びの履歴を記録（運搬担当者、運搬物等）、個人情報が記録された機器・電子媒体等は、データの暗号化又はパスワードにより保護等を行ったことを確認、書類等を持ち運ぶ際には処置（封筒への封緘、目隠しシールの貼付等）を行います。
- 事務取扱責任者は、個人情報の情報漏えいを防止するために、事務取扱担当者の役割や責任に応じて、データベース、フォルダ、ファイル等のアクセス可能領域を限定的に設定していることを確認、情報システムにアクセス可能な機器は、IPアドレス等による端末接続制限により使用可能な機器を限定していることを確認、情報システムにアクセス可能な事務取扱担当者を、認証ID等により限定していることを確認、ID・パスワード及び専用ICカード等の共同利用を禁止し、事務取扱担当者の個々に付与していることを確認、なりすましを防ぐため、多要素認証を適用していることを確認することなど、情報システム及び特定個人情報ファイルへのアクセス制御、アクセス者の識別・認証等に関するの対策を講じます。

5.15 その他のリスク対策 (個人情報の管理に関して)

上記のほか、個人情報の管理に際して次の措置を講じています。

委託先の不正が起こらないか

- 利用目的の達成に必要な限度において、個人情報を扱う事務を第三者に委託する場合、当該委託において取り扱う個人情報の安全管理措置が講じられるよう、委託先の適切な選定、委託先の安全管理措置を遵守させるために必要な契約の締結、委託先における特定個人情報の取扱状況の把握など適切な監督を行います。

個人情報 that 誤って消去等されないか

- 保存期間内は定期的にデータバックアップを実施し、複数個所に保管します。利用目的の達成等により個人情報の保存の必要がなくなった場合で、法令により必要な一定期間の保存期間を経過した場合には、速やかに当該個人情報を削除または廃棄します。

不要な個人情報がいつまでも保管されないか、古い個人情報を誤って利用しないか

- 5.10「顔画像・特徴量を確実に削除するのか」参照。

5.16 その他のリスク対策 (全般に関して)

上記のほか、次の措置を講じています。

点検・監査等

- NECではPマーク及びISMS認証を取得しています。
- システム監査を年1回実施します。
- NECでは、個人情報保護管理者のほか、個人情報保護監査責任者を指定し、監査計画及び監査の実施を行います。

従業者教育

- NECでは、少なくとも年1回定期的に、かつ必要に応じて適宜、従業者への教育・啓発を行っています。

開示・訂正・利用停止請求

- 個人情報保護法に則って、X社にご請求いただくことになります。

問合せ対応

- NECでは、ユーザの方等からのお問合せに真摯に対応いたします。下記、お問い合わせ窓口までお問い合わせください。
<https://jpn.nec.com/site/privacy/index.html>

残存リスク

- スライド5.12～5.16は全てNECにおけるリスク対策を記載しています。X社・Y社におけるリスク対策についてはX社・Y社に確認する必要があります。

5.17 個人情報保護法への適合性（抜粋）

取得フェーズ

- 適正取得（個人情報保護法17条）
 - 申込者・利用者が本件顔パス入場を理解した上で申し込んだり利用できるように、下記の通り利用目的の通知等を行っています。利用者に理解していただいた上でセキュリティを確保した方法で個人情報を取得しており、適正取得しています。
 - 仮に要配慮個人情報が映り込んだ場合でも、個人情報保護法17条2項に従った取得です。

利用フェーズ

- 利用目的の特定・公表等（個人情報保護法15条・18条）
 - 本件顔パス入場は、NEC・X社・Y社ともに、事前に特定・公表している利用目的の範囲内です。
 - NEC・X社・Y社ともに、プライバシーポリシー等で利用目的を公表していますが、さらに加えて、顔パス入場申込サイトや顔パス入場ゲートでも、利用目的の通知を行います。
- 目的内利用（個人情報保護法16条）
 - 本件は、事前に特定・公表している利用目的の範囲内の利用です。
 - 加えてNEC・Y社においては、委託の範囲内の利用です。

提供フェーズ

- 第三者提供（個人情報保護法23条）
 - 個人情報保護法23条に反した個人データの第三者提供は行いません。

6 総括

6.1 まとめ

- 本評価において、以下の項目について検討し、プライバシー等への影響を確認しました。

- ・ スキーム（1.1,1.2,2.1,2.2,4,5.4参照）
- ・ 個人情報の取扱い（7.1参照）
- ・ 個人情報利活用の効果（2.1参照）
- ・ 個人情報保護のポイント（3参照）
- ・ なりすまし対策（5.1参照）
- ・ 誤認証・誤認識対策（5.2参照）
- ・ 顔画像提供の任意性（5.3参照）
- ・ 個人情報不正利用リスク対策（5.5参照）
- ・ 個人情報の漏えいリスク対策（5.6,5.7参照）
- ・ 個人情報不適正取得リスク対策（5.8参照）
- ・ 個人情報不正提供リスク対策（5.9参照）
- ・ 個人情報未消去リスク対策（5.10参照）
- ・ プライバシー権侵害・監視リスク対策（5.11参照）
- ・ 個人情報の取得リスク対策全般（5.12参照）
- ・ 個人情報の利用リスク対策全般（5.13参照）
- ・ 個人情報の提供リスク対策全般（5.13参照）
- ・ 個人情報の管理リスク対策全般（5.14,5.15参照）
- ・ 個人情報のその他のリスク対策（5.16参照）
- ・ 個人情報保護法への適合性（5.17参照）

■ 評価実施手続

- ・ 本評価は世界各国のPrivacy Impact Assessment (PIA)や日本の法制等を参考にして、弁護士水町雅子が評価項目を決定しています。
- ・ NECから資料提供やヒアリングを受けながら弁護士水町雅子が実施しました。

6.2 水町雅子のコメント

最後に、弁護士水町雅子の意見を次のとおり、述べます。

- 顔認証技術は、より豊かで便利な社会を実現する期待・可能性を有する一方で、プライバシー権侵害の危険性も同時にはらみます。具体的に誰がどのような管理方法で、またどのようなセキュリティ対策を講じて顔写真データや特徴量を保持するのか、顔写真データや特徴量データを具体的にどのように利用し、どのような利用目的で利用するのか、外部提供は発生するのか等々、個人情報・プライバシー等への影響とその対策についての明瞭・透明かつ具体的な説明がなされることが大変重要であると考えます。プライバシー等の人々の権利利益に対する影響を様々な角度から事前に検討し、十分な対策を予め講じておくことは、個人情報やプライバシー権の保護をまずもっての大前提とした上で、適法・適正に新しい技術を活用していくために大きな意義があると考えます。
- 本件顔パス入場は、本人の明示的な同意に基づき、希望者のみが利用し、また目的が限定されていて、顔写真データや特徴量も顔パス入場のためだけに利用するスキームであり、他の顔認証技術の活用手法と比べても、比較的社会受容性も高いと考えられます。
- 顔認証技術を世界的にも展開しているNECが、「個人情報・プライバシー等保護」と「顔認証技術の活用」を両立させ、このようなPIAを実施することは大変意義深いことであり、顔認証以外の様々な分野における新技術の活用・導入にとっても、PIAの手法は有用であると考えます。今回、本評価に登場するX社・Y社は仮の企業でしたが、実際に顔認証技術を利用する企業においても広く、このPIAを参考にして、個人情報・プライバシー等保護を徹底するための施策・運用等を行っていただければ、非常に良いと思います。
- 顔認証技術は海外動向・海外規制、正答率、人権への影響等、様々な観点から、現在も変動している環境下にあります。今後も、様々な観点からのチェックを行い、社会に受け入れてもらえる適正な方法での活用を行っていただければと思います。

7 参考

- 7.1 パーソナルリファレンスアーキテクチャ
「顔認証機能を利用した催事等入場管理パーソナルデータリファレンスアーキテクチャ」
- 7.2 本評価書と特定個人情報保護評価書との対照関係
- 7.3 参考URL

7.1 パーソナルリファレンスアーキテクチャ「顔認証機能を利用した催事等入場管理パーソナルデータリファレンスアーキテクチャ」

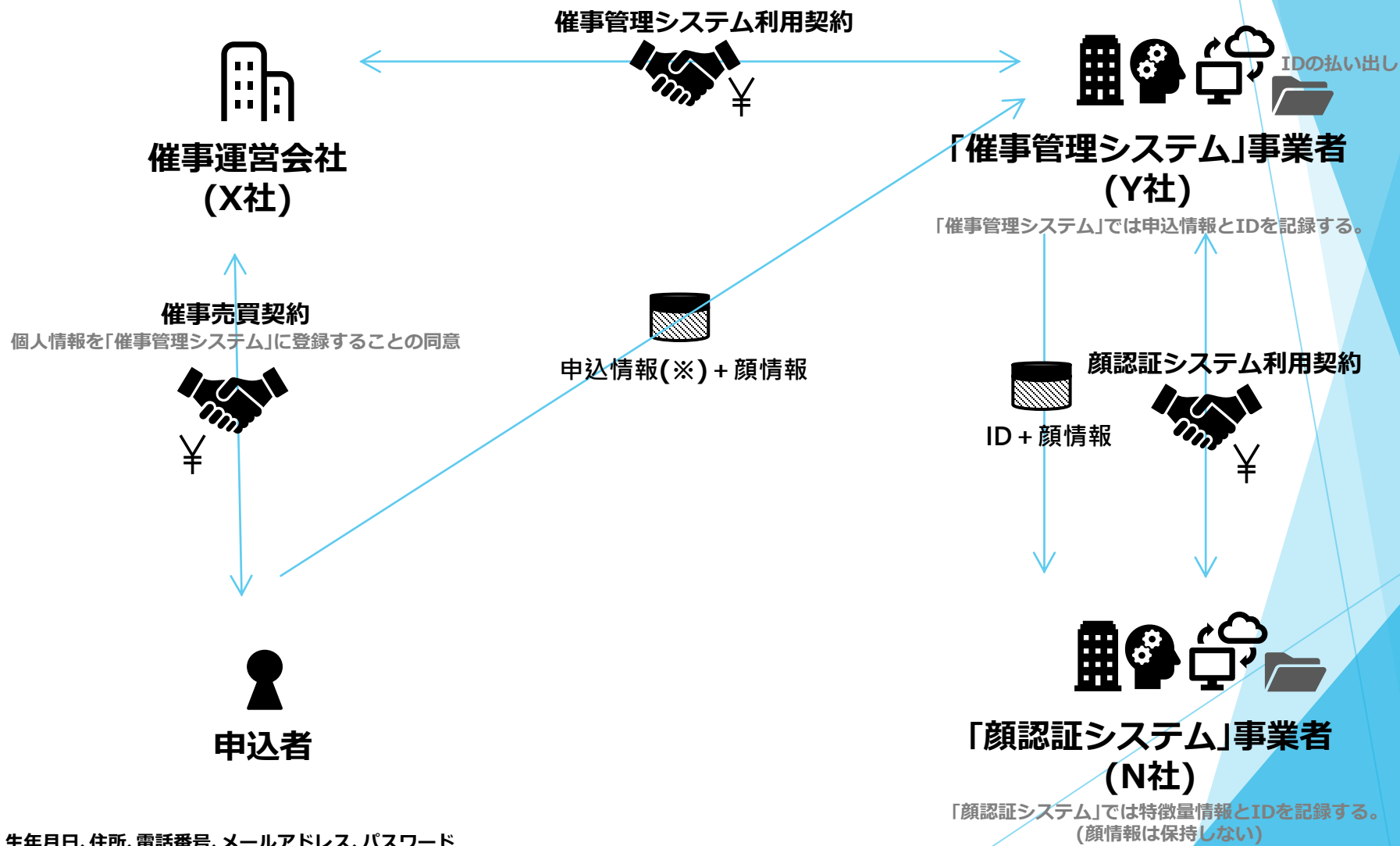
次ページ以降ご参照

1. ステークホルダリスト

名称	概要	ISO/IEC 29100での分類
申込者(エンドユーザ)	Webでイベント申込時に申込情報を提供する。	PII principal (データ主体)
催事運営会社(X社)	申込者から提供された申込情報を蓄積管理する。申込情報を管理蓄積するシステム運用と管理は、催事管理システム事業者(Y社)へ委託する。 個人情報保護法上の個人情報取扱事業者に該当。	Data controller (データ管理者)
「催事管理システム」事業者(Y社)	催事運営会社(X社)から申込情報の管理を受託し、X社に催事管理システムをクラウドサービスで提供する。 個人情報保護法上の委託先に該当。 また、催事管理システムが提供する機能のうち、顔認証情報を管理蓄積するシステム運用と管理は、顔認システム事業者(N社)へ委託する。	Data processor (データ処理者)
「顔認証システム」事業者(N社)	催事管理システム事業者(Y社)から顔認証情報の管理を受託し、Y社に顔認証システムをクラウドサービスで提供する。 個人情報保護法上の委託先(再委託先)に該当。	Data processor (データ処理者)
催事設備会社	催事会場に、催事管理システムと連動するカメラやフラッパーゲート等といったハードウェア設備を設置する。	非該当 (PII扱わない)

2. ビジネス関係

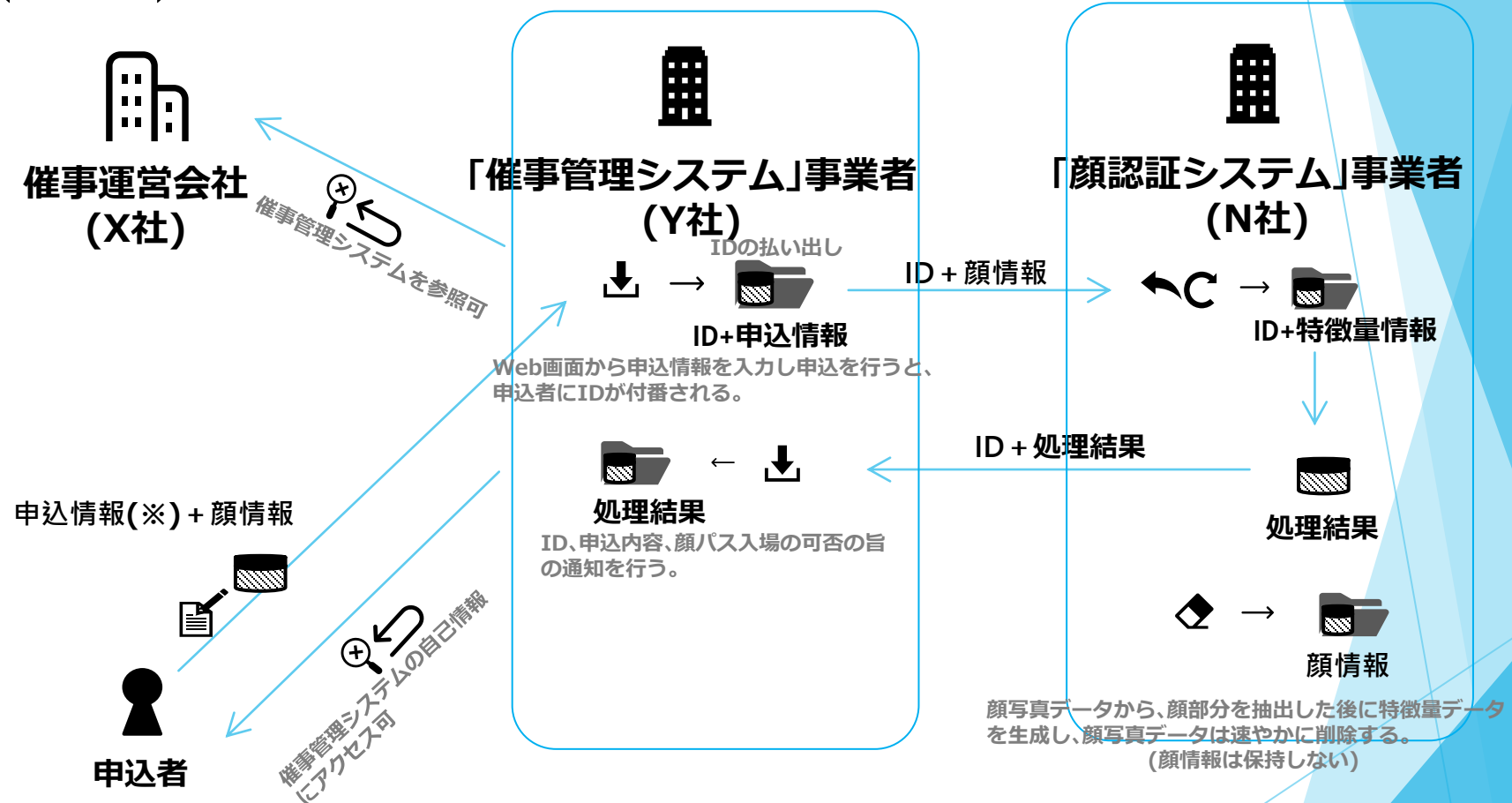
関与する個人、事業者間のビジネス関係(契約など)を明確化する



3. データリソースマップ

パーソナルデータを含むデータセットがどこに存在するのかを明確にする

申込時(顔登録)

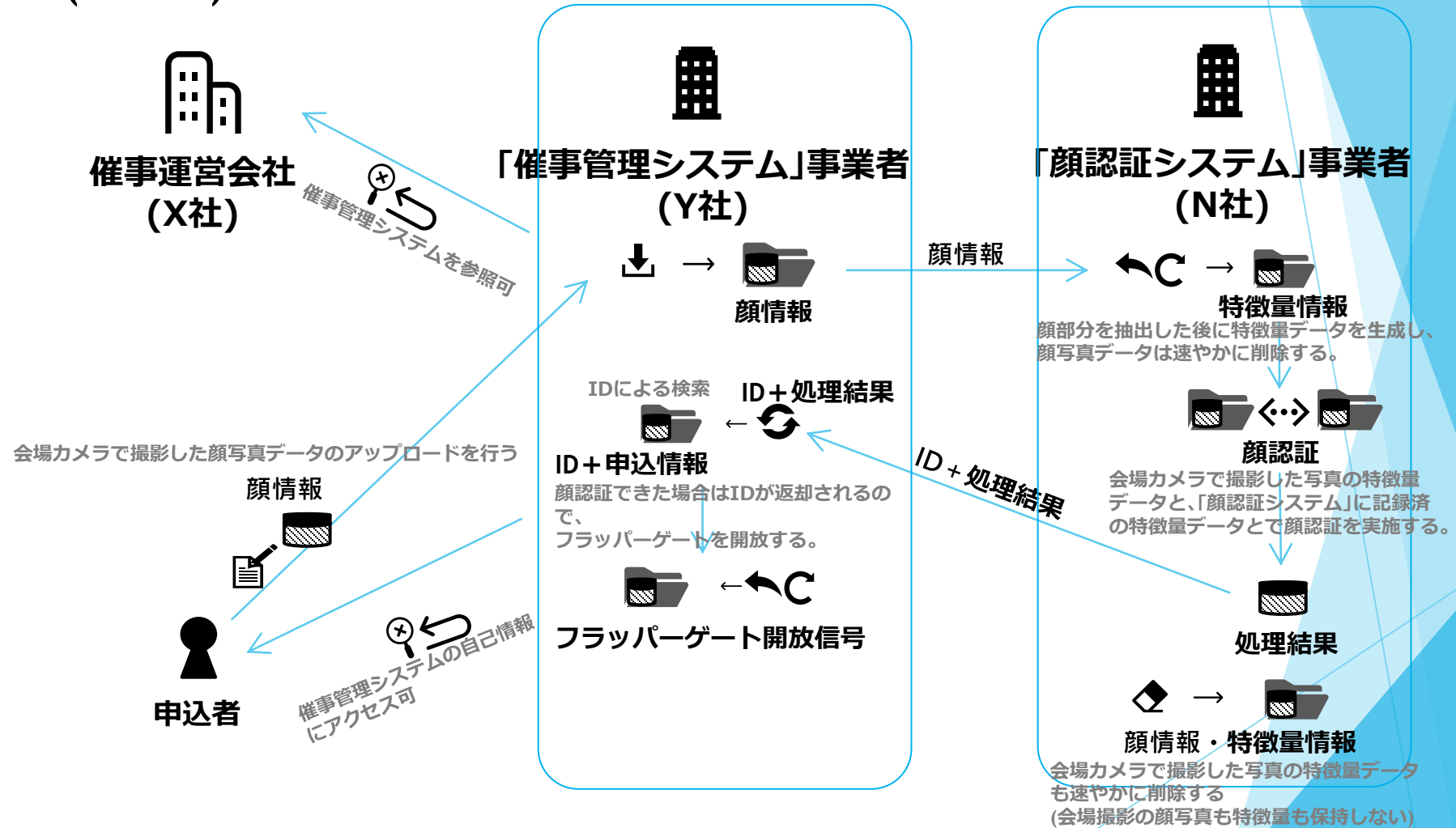


※:氏名、生年月日、住所、電話番号、メールアドレス、パスワード

3. データリソースマップ

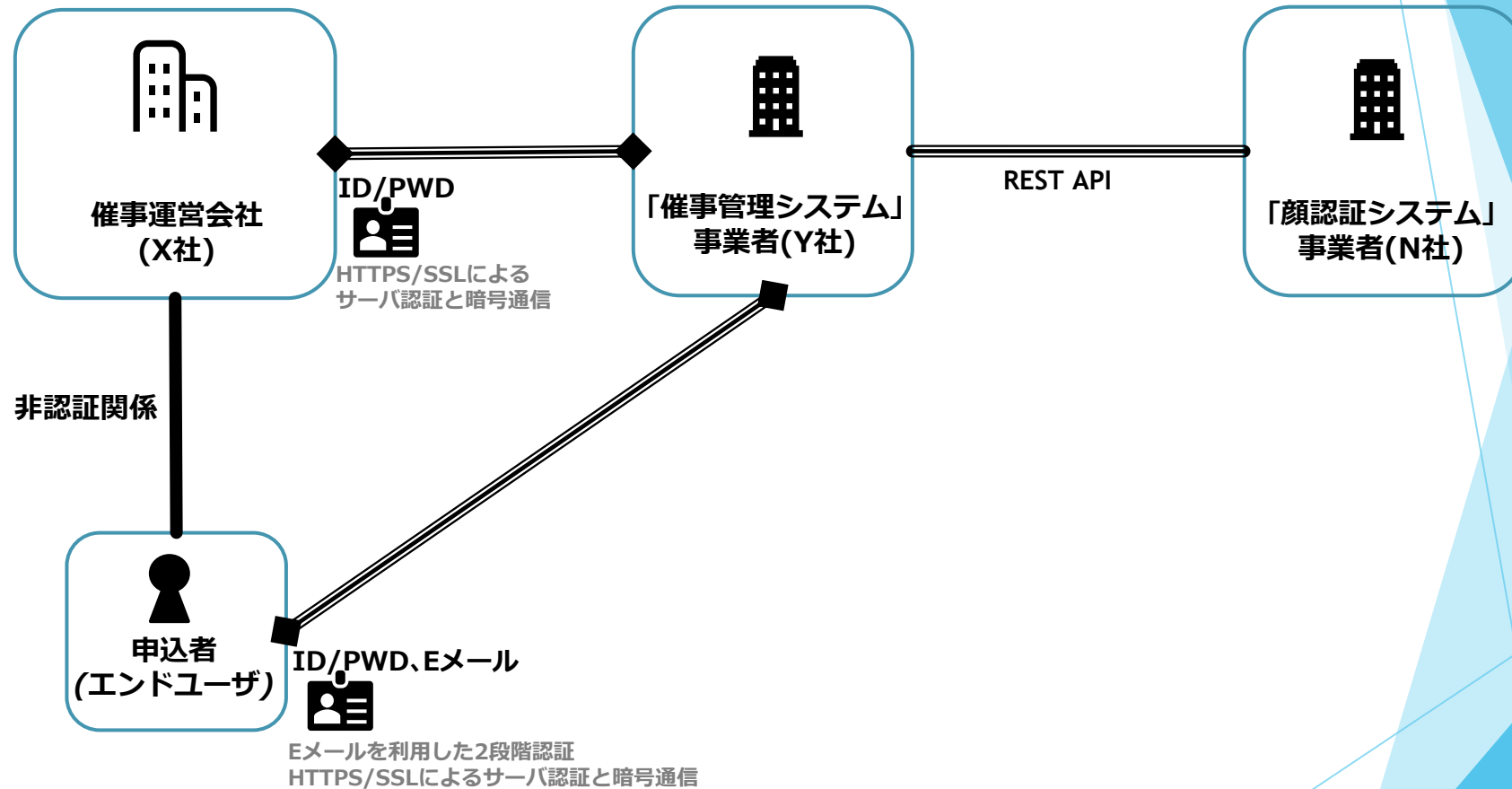
パーソナルデータを含むデータセットがどこに存在するのかを明確にする

入場時(顔認証)



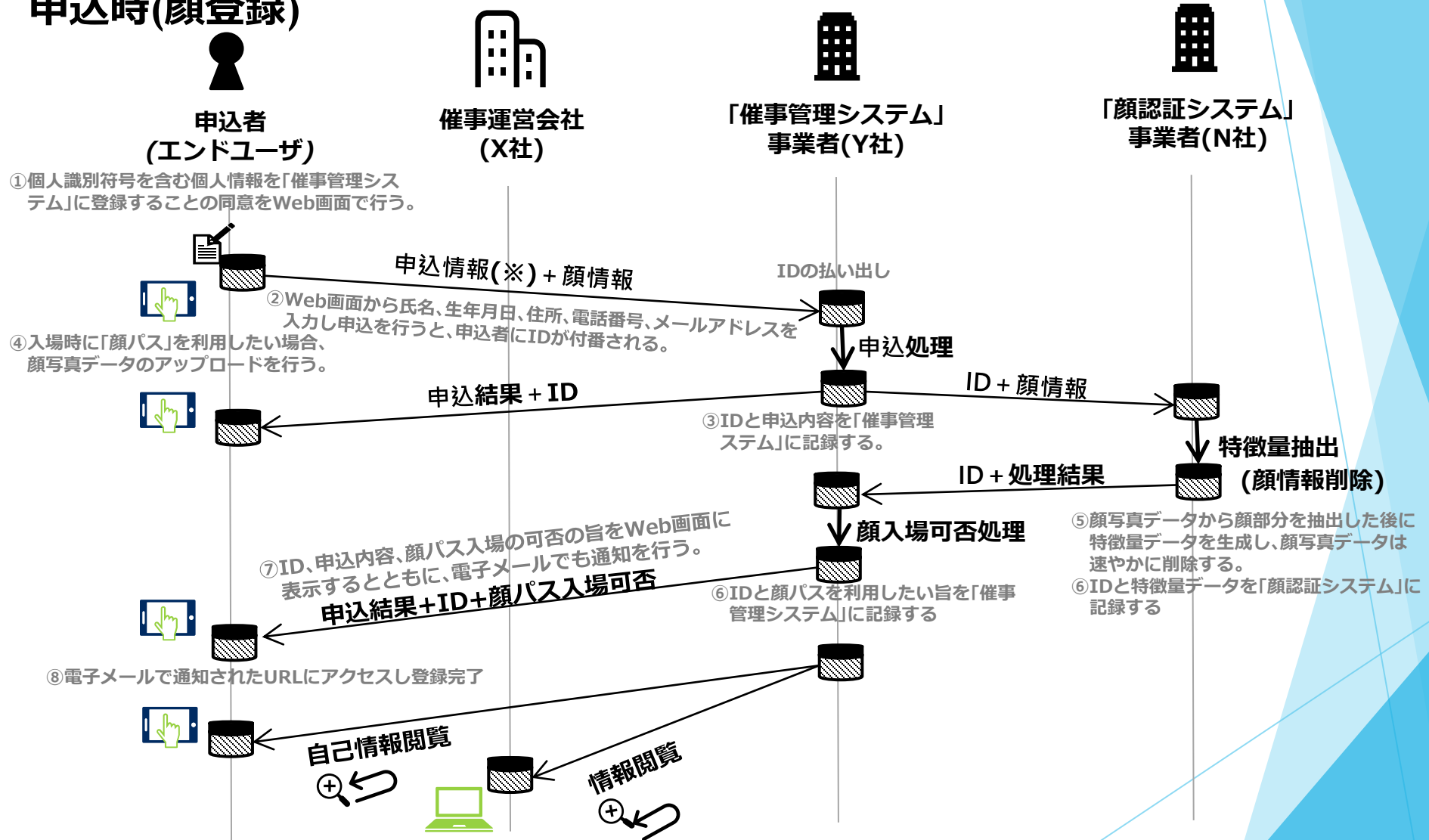
4. トラストリソースマップ

関係者間の認証・認可の関係を明確にする



5. データフローシーケンス

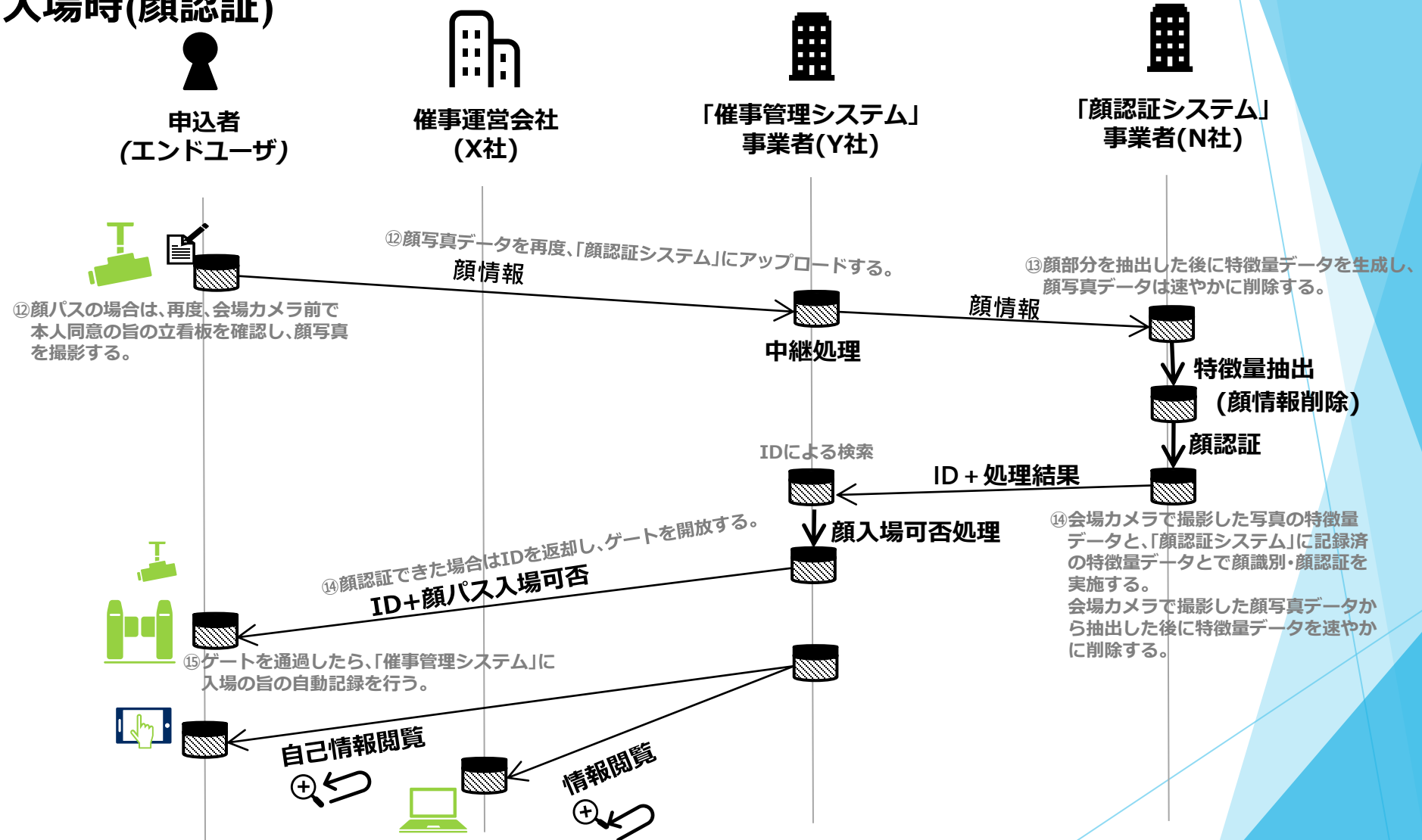
申込時(顔登録)



※:氏名、生年月日、住所、電話番号、メールアドレス、パスワード

5. データフローシーケンス

入場時(顔認証)



5. データフローシーケンス

No.	場面	機能要件	入力	記録	出力
1	申込	個人識別符号を含む個人情報を「催事管理システム」に登録することの同意をWeb画面で行う。同意した場合のみ申込者登録へ進む。	本人同意		
2	申込	Web画面から氏名、生年月日、住所、電話番号、メールアドレス、希望パスワードを入力し申込を行うと、申込者にIDが付番される。	申込者の個人情報		ID
3	申込	IDと申込内容を「催事管理システム」に記録する。		申込者の個人情報とID	
4	申込	入場時に「顔パス」を利用したい場合は、顔写真データを「催事管理システム」に登録することの同意をWeb画面で行う。同意した場合のみ顔写真データのアップロードへ進む。	本人同意		
5	申込	Web画面からIDと顔写真データのアップロードを行うと、顔部分を抽出した後に特徴量データを生成し、顔写真データは速やかに削除する。	顔写真		特徴量
6	申込	IDと特徴量データを「顔認証システム」に記録するとともに、IDと顔パスを利用したい旨を「催事管理システム」に記録する。		特徴量とID、顔パス可否	
7	申込	ID、申込内容、顔パス入場の可否の旨をWeb画面に表示するとともに、電子メールでも通知を行う。			電子メール
8	申込	電子メールで通知されたURLにアクセスすることで登録完了となる。	確認	確認完了	
9	取消	Web画面から、申込時のIDとパスワード、生年月日を入力し、「申込取消」のメールを要求する。	ID、生年月日		電子メール
10	取消	「催事管理システム」から「申込取消」の電子メールが通知されるので、電子メールで通知されたURLにアクセスすることで取消を行う。	確認	取消完了	
11	取消	取消が行われた場合には「顔認証システム」から「特徴量データ」を速やかに削除し、「催事管理システム」からは、「(顔パスを含む)申込内容」を速やかに削除する。問合せ対応のためIDだけは取消済のIDとして記録し保持しておく。		申込者の個人情報、特徴量、顔パスの情報を削除	

5. データフローシーケンス

No.	場面	機能要件	入力	記録	出力
12	(顔)入場	顔パスの場合は、再度、会場カメラ前で本人同意の旨の立看板を確認し、顔写真を撮影し顔写真データを再度、「顔認証システム」にアップロードして識別・認証することの同意を行う。同意された場合のみウォークスルー用のゲートに進む。	本人同意		
13	(顔)入場	会場カメラで撮影した顔写真データのアップロードを行うと、顔部分を抽出した後に特徴量データを生成し、顔写真データは速やかに削除する。	顔写真		特徴量
14	(顔)入場	会場カメラで撮影した写真の特徴量データと、「顔認証システム」に記録済の特徴量データとで顔識別・顔認証を実施し、認証できた場合はIDを返却し、ゲートを開放する。会場カメラで撮影した顔写真データから抽出した後に特徴量データを速やかに削除する。	特徴量		認証結果、ID
15	(顔)入場	ゲートを通過したら、「催事管理システム」に入場の旨の自動記録を行う。	ID	入場済	
16	(顔以外)入場	顔パスを行わない場合、もしくは顔認証で結果がエラーになった場合は、申込時に送付された電子メールもしくはWeb画面からIDを提示し、あわせて、顔写真付の身分証明書を提示することで、会場職員が「催事管理システム」を検索して確認を行い、会場職員がゲートの開放を行う。	ID		申込者の個人情報とID
17	(顔以外)入場	入場者がゲートを通過したら、会場職員がゲートを閉め、会場職員が「催事管理システム」を操作して入場の旨の記録を行う。	ID	入場済	

6. 法制関係図

	申込者(エンドユーザ)	催事運営会社(X社)	「催事管理システム」事業者(Y社)	「顔認証システム」事業者(N社)
申込者(エンドユーザ)	NA	売買契約等 個人情報に関する同意 個人情報保護法	個人情報保護法	個人情報保護法
催事運営会社(X社)	売買契約等 個人情報に関する同意 個人情報保護法	NA	委託契約 個人情報保護法	必要かつ適切な監督 個人情報保護法
「催事管理システム」事業者(Y社)	個人情報保護法	委託契約 個人情報保護法	NA	委託契約 個人情報保護法
「顔認証システム」事業者(N社)	個人情報保護法	必要かつ適切な監督 個人情報保護法	委託契約 個人情報保護法	NA

7.2 本評価書と特定個人情報保護評価書との対照関係

- 別添ご参照

https://www.miyauchi-law.com/f/210812necpia_taishou.pdf

7.3 参考URL

NEC顔認証

- <https://jpn.nec.com/biometrics/face/index.html>

他のPIAの例等

- 民間企業における医療情報を利用したサービスに関するPIAの例
<http://www.miyauchi-law.com/f/180327PIA.pdf>
のうちの9～32ページ
- 自治体における行政情報を活用した施策に関するPIAの例
https://www.soumu.go.jp/main_content/000620329.pdf
- 自治体における行政情報を活用した施策に関する全項目評価活用の例
https://www.nishi.or.jp/shisei/seisaku/johokasuishin/pia-jstorage.files/hyokasho_kekka.pdf
http://www.miyauchi-law.com/f/201002nishinomiya_pia.pdf
- 宮内・水町IT法律事務所PIA解説ページ
<http://www.miyauchi-law.com/dpia.html>

パーソナルデータリファレンスアーキテクチャ

- https://data-trading.org/sipb-1_personaldataarchitecture_dta/