Vol.2017-IS-141 No.8
2017/8/26

顔認識を用いる Glassware のための プライバシー保護ツールキット

岩崎 誠[†1]　掛下 哲郎[†2]

概要：Google は Google Glass（Glass）での顔認識技術の使用を禁止している．Glass はウェアラブルデバイスなので，写真や動画の撮影が気づかれにくく，プライバシー侵害に関する懸念の声が上がっていることが原因である．本論文では，個人情報保護の基本となるガイドラインとして OECD 8 原則を採用し，顔認識を用いる Glassware および Glassware で収集した個人情報を利活用する Web アプリケーションに OECD 8 原則を遵守させるためのプライバシー保護ツールキットを提案する．このツールキットは，Glassware 用ツールキットと Web アプリケーション用ツールキット，管理アプリケーションの 3 つで構成されている．Glassware 用ツールキットは，被認識者に関連する情報を取得・表示する Glassware に組み込むことを想定して開発しており，顔認識機能，ログ収集機能，ログ保存機能，ログ保存の許可申請機能，認識結果取得機能を提供する．Web アプリ用ツールキットは，収集したログの参照，変更，分析を行う Web アプリに組み込むことを想定して開発しており，画像ログ参照機能，その他ログ参照機能，ログ削除・ログ更新申請機能を提供する．管理アプリケーションは，ユーザーやアプリケーション，ログを管理するアプリケーションである．

キーワード：Google Glass，プライバシー保護，ツールキット，OECD 8 原則，顔認識

A Privacy Protection Toolkit for Glassware with Face Recognition

Makoto Iwasaki[†1]　Tetsuro Kakeshita[†1]

Abstract: Google prohibits using face recognition with Google Glass (Glass) because of the privacy problem. It is difficult for people to recognize capturing using video or still image because Glass is a wearable device. In this paper, we utilize OECD privacy guidelines as fundamental principles for privacy protection and propose a privacy protection toolkit for Glassware using face recognition and Web application utilizing privacy information collected by the Glassware. The toolkit is composed of a toolkit for Glassware, a toolkit for Web application and the administration application. A third-party Glassware is required to call functions, provided by the toolkit for Glassware, such as face recognition, log collection, storing of a log record, getting permission from a user to store a log record, and acquisition of face recognition result. A third-party Web application willing to utilize the collected log records is required to call functions, provided by the toolkit for Web application, such as reading the collected log records and images together with apply functions to update or delete a specified log record. The administration application provides administration functions of the users, registered applications and log records.

Keywords: Google Glass, Privacy Protections, Toolkit, OECD Privacy Guidelines, Face Recognition

1. はじめに

Google が開発する眼鏡型のウェアラブルデバイスである Google Glass(Glass) に顔認識技術を適用すると，様々な応用範囲の拡張が期待できる．

しかし, Google は 2013 年 6 月 1 日から適切なポリシーが策定されるまで Glass での顔認識技術の使用を禁止している[1]．眼鏡型のウェアラブルデバイスなので，Glass を用いた写真や動画の撮影が気づかれにくく，プライバシー侵害の懸念の声が上がっていることが原因である．また，2015 年 1 月 15 日には Glass の販売を中断することを発表している[2]．フォレスターの調査によると，消費者の 43% が Glass に関心を持っていた一方，それを上回る消費者がプライバシーの問題に懸念を持っていたという．

OECD（経済協力開発機構）は 1980 年に個人情報保護の基本となるガイドライン「OECD 8 原則」を定め，2013 年に更新版を勧告した[3]．これは，世界の個人情報保護の共通した基本原則となるもので，日本の「個人情報保護法」も「OECD 8 原則」に準拠した形で制定されている．「OECD 8 原則」は，目的明確化の原則，利用制限の原則，収集制限の原則，データ内容の原則，安全保護の原則，公開の原則，個人参加の原則，責任の原則の 8 つからなる．プライバシーを保護した Glassware を開発するには，これらの原則を遵守する必要がある．

そこで，本研究では，顔認識を用いる Glassware のためのプライバシー保護ツールキットの企画及び基本機能の開発を行った．このツールキットは，教員と学生，上司と部下，店員と顧客など，多くの人に関わるユーザー向けに，被認識者に関連する情報を収取する Glassware や，収集された個人情報を利活用する Web アプリケーションに組み込むことを想定して開発しており，OECD 8 原則に対応した機能を組み込むことで，プライバシーを保護している．

†1 佐賀大学 工学系研究科 知能情報システム学専攻
Graduate School of Information Science, Saga University

本ツールキットを用いることで，撮影された個人に通知を出すことで了解を求め，了解を受けた認識結果のみを表示･保存することができる. このツールキットは, Glassware 用ツールキットと Web アプリ用ツールキット, 管理アプリケーションの 3 つで構成されている. Glassware 用ツールキットは，被認識者に関連する情報を取得・表示する Glassware に組み込むことを想定して開発しており, 顔認識機能，ログ収集機能，ログ保存機能，ログ保存の許可申請機能，認識結果取得機能を提供する．Web アプリ用ツールキットは，収集したログの参照，変更，分析を行う Web アプリに組み込むことを想定して開発しており，画像ログ参照機能，その他ログ参照機能，ログ削除・ログ更新申請機能を提供する．管理アプリケーションは，ユーザーやアプリケーション，ログを管理するアプリケーションである．

本論文では，顔認識のためのプライバシー保護ツールキットの企画及び基本機能の開発を行ったので，これについて報告する．2 節では，本研究で使用する Glass のハードウェアと機能，顔認識技術の適用事例を紹介する．3 節では OECD 8 原則を紹介する．4 節では，本研究で企画，開発したプライバシー保護ツールキットの構成および管理するデータを示す．5 節では，ツールキットの機能を示し，6 節でツールキットの処理の流れを説明する．これらに基づいて 7 節では本ツールキットが OECD 8 原則を遵守することを示す．8 節ではツールキットの実装について述べる．

2. Google Glass

2.1 ハードウェア

Google Glass（Glass）とは，Google が開発する眼鏡型のウェアラブルデバイスである．Glass のハードウェア構成は，ディスプレイ，カメラ，マイク，タッチパッド，スピーカー，9 種のセンサーである．カメラの解像度は 500 万画素，動画は 720p で撮影でき，iPhone4 と同等の性能がある．

2.2 機能

Glass で使う一列に並んだカード型の UI をタイムラインと呼ぶ. カードの挿入位置によって, 情報の内容が異なる. カードをタップすることでメニューアイテムが表示され，動作をスワイプで選択できる．

Home カードが表示された状態で「OK glass」と発声すると，音声コマンドの候補がディスプレイに表示される．続けて音声コマンドを発声することで，方向案内やメッセージ送信，電話などのコマンドに対応するアプリケーションを起動できる．

2.3 顔認識アプリケーション

Glass に顔認識技術を適用した事例として，Name Tag アプリ，感情認識アプリ，自閉症治療アプリ，ドバイ警察での犯罪捜査などが挙げられる．

Facial Network 社が開発している Name Tag アプリは，顔認識機能を用いて，氏名・交際ステータス・学歴・職業や趣味・性犯罪履歴などを検索できる[4].

また，顔認証技術で知られる企業 Emotient 社が開発している感情認識アプリは，感情をリアルタイムで読み取る機能を提供する[5]．集団や個人の感情の変化を数値化し，感情を読み取ることができる．小売店の売り場で活用し，販促やプロモーションの現場で，顧客に満足を与えられたかを数値化する，ヘルスケアの分野でうつ病を検出するといった利用法が想定されている．

また，Brain Power 社が開発している自閉症治療アプリケーションは，自閉症の症状を適切に評価し，継続的に観察する．さらに，ゲームを通じて表情の認識トレーニングが実施できるほか，メルトダウンと呼ばれるパニック症状の発症を予測し，両親や介護者に知らせる機能も持つ[6].

ドバイ警察の犯罪捜査では，同国の捜査機関が開発した専用の顔認識ソフトを用いて，操作現場で容疑者の写真を即座にデータベースと照合し，犯罪捜査に役立てている[7].

3. OECD 8 原則

OECD 8 原則は, 以下の 8 つの原則から構成される. なお, 本ツールキットでは，責任の原則を除く 7 つの原則を実装し，責任の原則はツールキット管理者が担保する．

- 目的明確化の原則

個人データの収集目的を明確にし，データ利用は収集目的に合致するべきである．

- 利用制限の原則

データ主体（個人情報の持ち主）の同意がある場合や法律の規定による場合を除いては，収集したデータを目的以外に利用してはならない．

- 収集制限の原則

個人データは，適法・公正な手段により，かつ情報主体に通知または同意を得て収集されるべきである．

- データ内容の原則

収集する個人データは, 利用目的に沿ったもので, かつ, 正確・完全・最新であるべきである．

- 安全保護の原則

合理的安全保護措置により，紛失・破壊・使用・修正・開示等から保護すべきである．

- 公開の原則

個人データ収集の実施方針等を公開し，データの存在，利用目的，管理者等を明示するべきである．

- 個人参加の原則

自己(データ主体)に関するデータの所在及び内容を確認

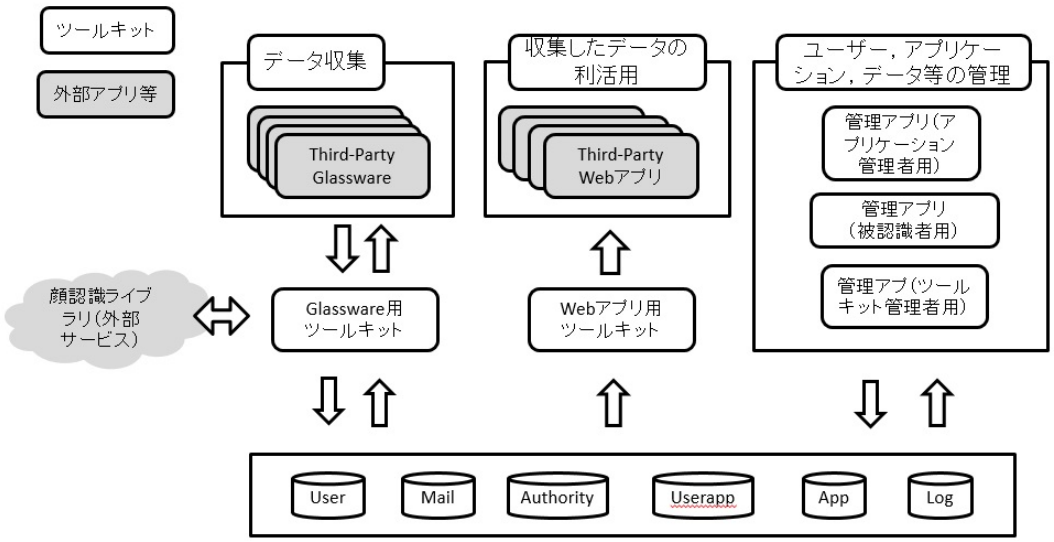


図 1：システム構成

させ，または異議申立を保証するべきである．

- 責任の原則

個人データの管理者は諸原則を実施する責任を有する．

4. プライバシー保護ツールキット

4.1 ユーザー

ツールキットの利用者は認識者，被認識者，アプリケーション管理者, ツールキット管理者の 4 種類に分類できる．

認識者はツールキットに登録した Glassware を使って個人情報を収集する．また，ツールキットが提供する機能を用いて収集した情報を参照できる. Glassware が被認識者の個人情報を取得する際には，被認識者の同意を得る仕組みになっている．

被認識者は認識者から個人情報を収集されるが被認識者用に提供されている管理アプリケーションを使うことで, 収集された自己の情報を参照でき，必要に応じて訂正や削除を依頼できる．また，被認識者は，自己の個人情報を収集できる Glassware を指定することもできる．

アプリケーション管理者はツールキットを利用するアプリケーション（Glassware または Web アプリケーション）や認識者の登録，削除などをツールキット管理者に申請する．ツールキット管理者はアプリケーションやユーザーの登録，削除，ログデータの訂正などの申請に対応する．

4.2 全体構成

顔認識を用いる Glassware のためのプライバシー保護ツールキットは，図 1 に示すように，Glassware 用ツールキット，Web アプリ用ツールキット，3 種類の管理アプリケーションおよびデータベースから構成されている．2 つのツールキットと管理アプリケーションは HTTP サーバー上で稼働している．

Glassware 用ツールキットは，被認識者に関連する情報を収集する Glassware から呼び出すことを想定して開発しており，ログ収集機能，顔認識機能，ログ保存機能，許可申請機能，認識結果取得機能を提供する．

一方，Web アプリケーション用ツールキットは，収集された個人情報を参照する Web アプリや, 収集された情報の削除または更新を依頼するための Web アプリ向けの機能を提供する．Web アプリケーション用ツールキットは画像ログ参照機能，その他ログ参照機能，ログ更新・削除申請機能を提供する．

管理アプリケーションは，被認識者，アプリケーション管理者およびツールキット管理者に対して，ユーザーやアプリケーション, ログデータ等を管理する機能を提供する．

図 1 に示すように, Glassware が撮影した顔画像は顔認識 API を用いて個人識別されるが，その際には外部サービスを活用する．識別された個人情報は，被認識者の同意を確認した後, データベースに格納される. データベースには，ユーザー登録情報，アプリケーション情報，Glassware で収集した個人情報等が格納されている．

4.3 データベース

データベースには，ユーザー情報を保持する User，ユーザーが保有する複数のメールアドレスを保持する Mail，ログ情報に対する権限の種類を保持する Authority，被認識者が許可するアプリケーション情報を保持する Userapp，アプリケーション情報を保持する App，ログ情報を保持する Log の 6 つのテーブルがある．それぞれが保持する情報を以下に示す. 下線を引いているフィールドが主キーである．

User

- userid：ユーザーID
- password：パスワード
- name：ユーザーの氏名
- adminFlag : ユーザー種別（一般ユーザー，アプリケーション管理者，ツールキット管理者）

Mail
- userid：ユーザーID
- eMailAddress：メールアドレス

Authority
- Authcode：権限コード
- AuthName：権限の種類（認識者，被認識者，管理者）

Userapp
- userid：ユーザーID
- appid：ユーザーが許可するアプリケーションの ID
- authcode：権限コード

App
- appid：アプリケーション ID
- password：パスワード
- appname：アプリケーションの名前
- purpose：被認識者情報を利用する目的
- time：日付・時刻を利用する目的
- image：画像を利用する目的
- location：場所を利用する目的

Log
- number：ログナンバー
- recognizer：認識者のユーザーID
- recognized：被認識者のユーザーID
- appid：アプリケーションの ID
- dateAndTime：画像を撮影した日付・時刻
- imagePath：保存した撮影画像のファイルパス
- location：撮影場所の位置情報（住所等）
- flag：応答フラグ

5. ツールキットの機能

本ツールキットは，管理アプリケーション，Glassware 用ツールキット，Web アプリケーション用ツールキットの 3 つで各種の機能を提供する．管理アプリケーションは，Web アプリケーションとして UI（ユーザインタフェース）まで実装した状態で提供する．一方，Glassware 用ツールキットと Web アプリケーション用ツールキットはライブラリとして開発されており，顔認識機能の呼び出し，ログデータに対する操作，およびアクセス制御機能を提供する．サードパーティの Glassware や Web アプリケーションの UI 等は，それぞれ専用のライブラリを活用して実現するのが合理的と考えられる．

5.1 管理アプリケーション

5.1.1 被認識者用アプリケーション

- ログイン・ログアウト機能
- アプリケーション選択機能：被認識者が顔認識を許可する Glassware を選択できる機能
- ログ保存の許可申請への対応機能：許可申請機能で申請されたログデータの保存の可否を選択できる．
- ユーザー情報参照機能：氏名やメールアドレスなどのユーザー情報を参照する機能
- ログ参照機能：被認識者に関連するログを参照する機能
- ログ更新・削除申請機能：被認識者に関連するログの更新または削除をツールキット管理者に申請する機能

5.1.2 ツールキット管理者用アプリケーション

- ログイン・ログアウト機能
- ユーザー登録・更新・削除機能：ツールキットを利用するユーザーを登録・更新・削除する機能
- アプリケーション登録・更新・削除機能：ツールキットを利用するアプリケーションを登録・更新・削除する機能
- ログ参照・更新・削除機能：ログを参照・更新・削除する機能

5.1.3 アプリケーション管理者用アプリケーション

- 認識者権限設定機能

アプリケーションを用いてログの収集，分析を行うユーザーを登録できる．

5.2 Glassware 用ツールキット

- 顔認識機能

顔認識 API を用いて撮影画像から被認識者を特定し，ユーザーID を取得する．引数は画像とアプリケーションのパスワード，戻り値は被認識者のユーザーID のリストである．

- ログ収集機能

ログ保存機能で利用するログを Glassware から収集する機能．画像，位置情報，認識者 ID,アプリケーション ID を取得する．

- ログ保存機能

認識者 ID，被認識者 ID，画像，位置，日付・時刻，アプリケーション ID をデータベースに保存できる．

引数は認識者 ID，被認識者 ID，画像，位置，日付・時刻，アプリケーション名で，戻り値はログナンバーである．ログナンバーは許可申請機能で送信するメールに記載する．

- ログ保存の許可申請機能

許可申請機能は，被認識者に対して，ログデータの保存を申請する機能である．データベースから認識者の氏名と被認識者の氏名，メールアドレスを取得し，ツールキットから被認識者にメールで保存の許可を申請する．通知することで，Glass を用いた撮影に気づきにくい欠点の軽減を図っている．また，被認識者が通知を受け取る際に，即座に対応する必要がなく，開発するうえでデバイスの差異を考慮する必要がないメールで通知している．

引数はログナンバー，戻り値はない．

- 認識結果取得機能

被認識者の氏名や画像，撮影された位置・時刻・日付などの認識結果を取得する．

引数はログナンバー，戻り値は，被認識者 ID，被認識者

の氏名，画像，位置，時刻・日付のリストである．

5.3 Web アプリケーション用ツールキット

認識者，被認識者などのユーザーや，アプリケーション毎にログの参照や更新・削除の申請ができる．

- 画像ログ参照機能

指定したアプリケーション，ログナンバーの画像を参照する．引数はアプリケーションのパスワード，ログナンバー，戻り値は画像ファイルの BufferedImage である．

- その他ログ参照機能

指定したアプリケーション，ユーザーに関連するログを参照する．引数はアプリケーションのパスワード，SQL 文の WHERE 句，戻り値はログレコードのリストである．

- ログ更新・削除申請機能

ログの更新・削除をツールキット管理者に申請できる．データ内容の正確性を確保するために管理者のみログの更新・削除ができるようにしている．

6. ツールキットの処理の流れ

本節では，ユーザーが，Glassware や Web アプリを介して本ツールキットの機能を利用する方法を説明する．

6.1.1 ツールキットの初期設定

ツールキットの設定では，ユーザー登録，アプリケーション登録を行うことができる．これらの機能は，管理アプリケーションが提供しており，Glassware を使った個人情報の収集や，収集した個人情報の利活用を行うに当たっての前提となる．本ツールキットでは，これらの機能は Web アプリから呼び出すことを前提としている．

ユーザー登録を行う際には，ツールキット管理者はユーザー登録機能を利用して，ユーザーID，パスワード，名前，メールアドレスを User・Mail テーブルに，顔画像とユーザーID，アプリケーション ID を顔認識 API にそれぞれ登録する．顔認識 API は，ここで登録した顔画像を用いて個人を識別する．

アプリケーションの登録を行う際には，ツールキット管理者は，アプリケーション登録機能を利用して，アプリケーション ID，アプリケーション名，時間や場所などの各ログ情報を利用する目的を App テーブルに登録する．本機能を用いて登録したアプリケーションのみ，ツールキットが保持するデータを利用できる．

ログを収集・分析するユーザーの登録を行う際には，アプリケーション管理者は，認識者権限設定機能を利用してユーザーID，アプリケーション ID，権限コードを Userapp テーブルに登録する．

被認識者が顔認識を許可するアプリケーションを登録する際には，アプリケーション登録機能を利用してユーザーID，アプリケーション ID，権限コードを Userapp テーブルに登録する．

6.1.2 Glassware を用いたログの収集

ツールキットを組み込んだ Glassware を用いてログを収集する．ログ収集のアクティビティ図を図 2 に示す．

1. ログの収集，保存

認識者は，Glassware でログ収集機能，ログ保存機能，許可申請機能，認識結果取得機能を利用して被認識者に関連する情報を取得する．だたし取得した個人情報は，被認識者の同意を得なければ保存・参照できない．

1.1. ログ収集

ログ収集機能を利用して，Glassware で画像，位置，時間等を取得し，HTTP サーバーに送信する．

1.2. 被認識者の特定

ツールキットでは，顔認識機能を利用して，撮影画像から被認識者のユーザーID を取得する．

1.3. 一時ログの保存

ログ保存機能を利用して，ツールキットで受信した画像，位置，時間などのログをデータベースに保存する．

1.4. ログデータ保存の許可申請

ログ保存の許可申請機能を利用して，データベースから被認識者のメールアドレスを取得し，ログ保存を申請するメールを被認識者に送信する．メールにはログの主キーを記載する．被認識者はメールを受信することで，Glass での撮影に気づくことができる．

1.5. 許可申請への対応

被認識者は，管理アプリケーションを用いて許可申請に対応できる．申請メールに記載されているログの主キーを用いてログを確認し，時間や場所などの各項目の保存の可否を選択する．拒否された項目はログから削除される．

2. Glass でのログの参照

認識者は，認識結果取得機能を利用して，ログ情報を Glassware で確認できる．

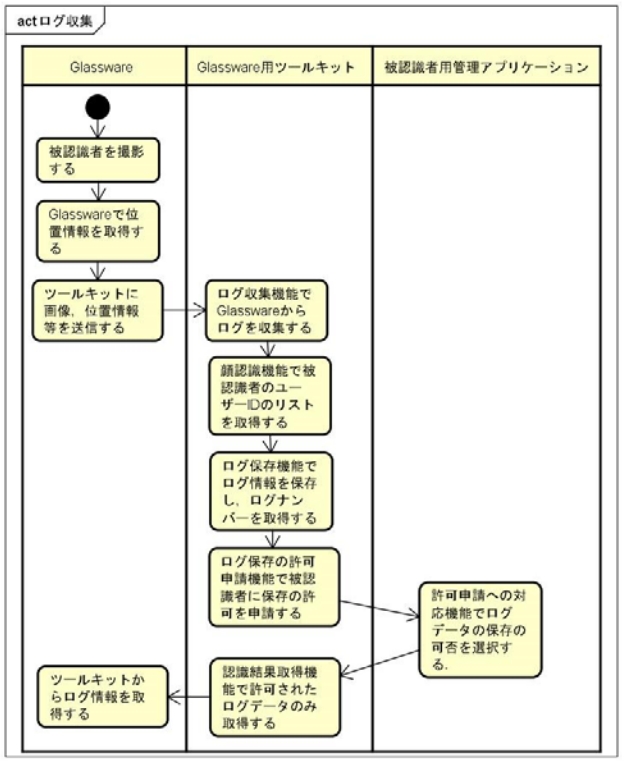


図 2：ログ収集のアクティビティ図

6.1.3 ログの参照・更新・削除

認識者，被認識者は，Web アプリで画像ログ参照機能，その他ログ参照機能, 更新･削除申請機能を利用することで，ログの参照や分析及び修正・削除申請ができる．

- 画像ログの参照

画像ログの参照のアクティビティ図を図 3 に示す．Web アプリケーションは，アプリケーションのパスワード，ログナンバーをツールキットに送信する．ツールキットではパラメーターを用いてログレコードを特定し，画像のファイルパスを取得する．ファイルパスから BufferedImage を作成し，Web アプリケーションに送信する．Web アプリケーションでは受信した BufferedImage を利用して画像ログを参照できる．

- その他のログの参照

その他のログの惨状のアクティビティ図を図 4 に示す．Web アプリケーションは, アプリケーションのパスワード, SQL 文の WHERE 句をツールキットに送信する．ツールキットではパラメーターを用いてログレコードを取得する．ログレコードを Json に変換し, Web アプリケーションに送信する．Web アプリケーションでは受信した Json を利用してログを参照できる．

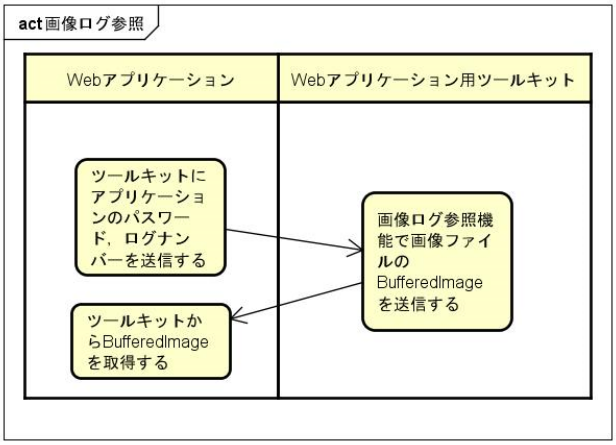
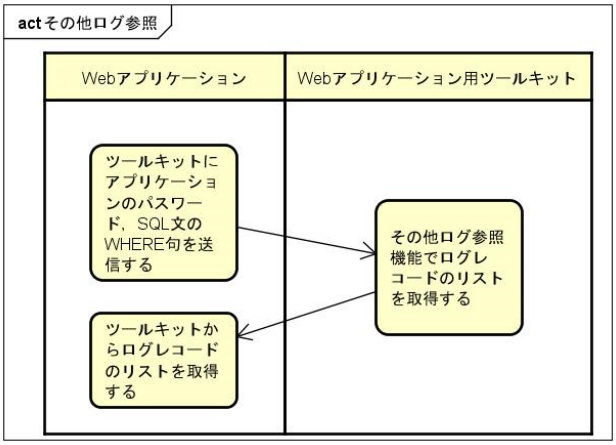
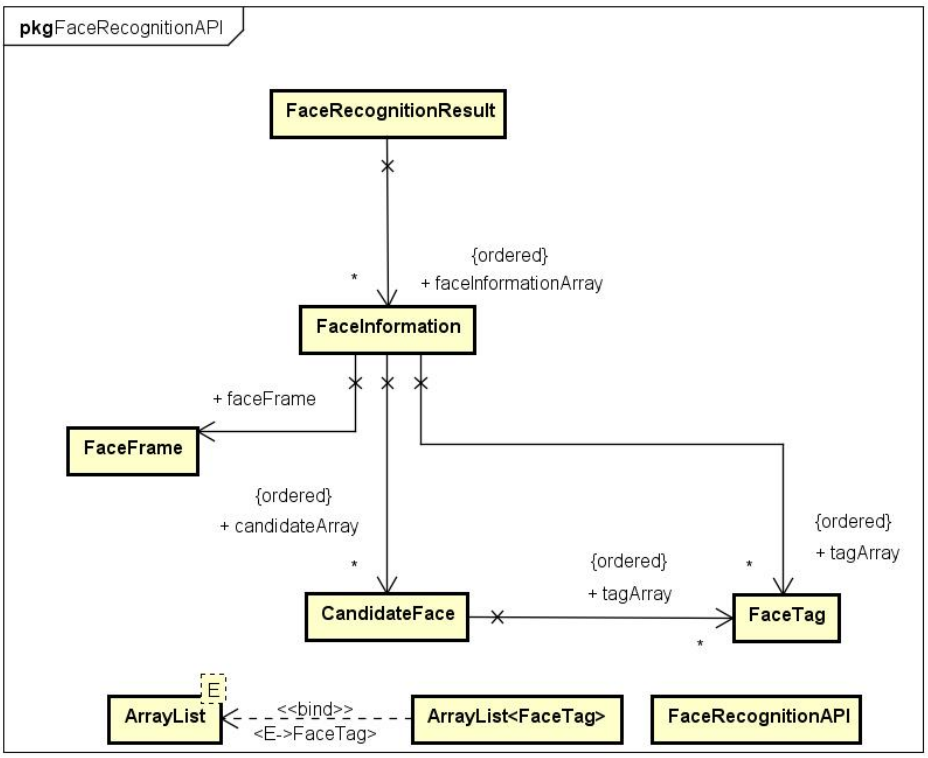


図 3：画像ログ参照のアクティビティ図



図：4 その他のログ参照のアクティビティ図



図：顔認識に関するクラス

7. ツールキットを用いた OECD８原則の実現

7.1 目的明確化の原則

アプリケーション登録機能で，App テーブルに被認識者情報，日付・時刻画像，場所毎に目的を登録することで，収集目的を明確にしている．

7.2 利用制限の原則

アプリケーション登録機能で登録する際に，アプリケーションが目的に沿って収集したデータを利用しているかをツールキット管理者が確認し，登録したアプリケーションのみツールキットを利用できる．また，アプリケーション選択機能で許可されたアプリケーションのみ個人情報を利用できる．

7.3 収集制限の原則

許可申請機能でデータ収集を通知し，申請許可機能で同意を得る．同意が得られない情報は削除され，同意が得られた情報のみ保存される．同意が得られた情報のみ認識結果取得機能を用いて Glassware 上で取得でき，画像ログ参照機能，その他ログ参照機能を用いて Web アプリケーション上で取得できる．

7.4 データ内容の原則

アプリケーション登録機能を用いることで，ツールキット管理者は収集する被認識者情報，日付・時刻，画像，位置情報毎に収集する目的が適切か確認できる．収集する被認識者情報については，顔認識 API の精度によっては誤判定する可能性があるが，誤った場合はログ更新，削除機能により修正することができる．

7.5 安全保護の原則

安全保護については，既存のセキュリティ技術を適用することで対応する．

7.6 公開の原則

被認識者は，アプリケーション選択機能で顔認識を許可するツールキットを選択する際にアプリケーションがログデータを利用する目的を確認でき，ログ参照機能で，自身に関するログを参照できる．

7.7 個人参加の原則

ログ取得機能にてデータの内容を開示できる権利を，ログ削除機能，ログ更新申請機能にて削除，訂正できる権利を保障している．

7.8 責任の原則

諸原則実地の責任はツールキット管理者が担保する．

8. 実装

8.1 顔認識 API

顔認識 API には, PUX WebAPI を利用している. これは，パナソニック株式会社の社内ベンチャー制度にて設立した PUX 株式会社の顔認識ソフトウェア FaceU ver.3 を利用した顔認識 API である． HTTP リクエストで API を利用し，XML または JSON 形式でレスポンスを取得する．

この API には，登録機能・認証機能・タグ編集機能・登録情報取得機能・登録情報削除機能の 5 つの機能がある．

登録機能は，画像ファイルから検出した顔をデータベースに登録する．そして，登録した顔を示す固有の番号（顔検出番号）を返す．認証機能は，画像ファイルから検出し

た顔をデータベースに登録された顔と認証する．タグ編集機能は，顔を識別するタグ情報を追加，更新，削除する．Key=value 方式の文字列として指定する．key のみ指定し，value を省略することもできる．1 つの顔に最大 10 のタグを設定できる．登録情報取得，削除機能は，画像やタグ等の登録情報を取得，削除できる．

Json 解析には，Json 処理ライブラリである Jackson Json Processor を利用した．このライブラリには，3 つの方法が提供されている．1 つ目は Streaming API で，データを順に読み込みながら処理する．特定の要素を取得するような用途には不向きである．2 つ目は Tree Model で，XML DOM のようにアクセスできる．3 つ目は DataBinding で，Json データを Java のデータ型と相互に変換できる．

8.2 クラス

8.2.1 顔認識に関するクラス

顔認識 API の画像登録，認証などの機能と，顔画像，認識結果などの情報を保持するクラスを以下に示す．

- FaceRecognitionAPI：顔認識 API の画像登録，認識などの機能を提供するクラスである．API の実行結果を Json で返す．
- FaceRecognitionResult：API の機能の実行結果を保持するクラスである．実行結果の json を引数にインスタンスを作成する．変数として FaceInformation の動的配列を保持する．
- FaceInformation：顔毎の API 実行結果を保持するクラスである．変数として FaceTag の動的配列，顔検出番号，登録画像への URL，顔の信頼値，FaceFrame，CandidateFace の動的配列を保持する．
- FaceFrame：画像の顔領域の矩形座標を保持する．
- FaceTag：登録した顔画像のタグ情報を保持する．
- CandidateFace：顔認識機能の結果を保持する．認証スコア，顔検出番号，FaceTag の動的配列を保持する．

8.2.2 管理アプリケーションに関するクラス

管理アプリケーションに関するクラスでは，ユーザーやアプリケーション，ログの登録や更新などの機能を提供する．ログインしたユーザーの権限に応じてデータベースへのアクセスを制御する．

- AddUser：ユーザー情報を追加する．ツールキット管理者のみ実行できる．
- GetUser：ユーザー情報を参照する．ツールキット管理者はすべてのユーザー情報を参照できる．
- UpdateUser：ユーザー情報を更新，削除する．ツールキット管理者のみ実行できる．
- AddApp：アプリケーションを登録する．ツールキット管理者のみ実行できる．
- GetApp：アプリケーション情報を参照する．ツールキット管理者は全てのアプリケーション情報を参照できる．
- UpdateApp：アプリケーション情報を更新，削除する．ツールキット管理者のみ実行できる．
- GetLog：ログ情報を参照する．ツールキット管理者は全てのログ情報を参照できる．
- UpdateLog：ログ情報を更新，削除する．ツールキット管理者はのみ実行できる．

8.2.3 Glassware 用ツールキットに関するクラス

- ToolKitForGlassware：受信した認識者のユーザーID，アプリケーションのパスワード，画像，位置情報に対して，顔認識，ログ保存の許可申請，ログ保存，ログの取得を行う．

8.2.4 Web アプリケーション用ツールキットに関するクラス

- GetImageLog：受信したアプリケーションのパスワード，ログナンバーに対して，画像の BufferedImage を取得する．
- GetOtherLog：受信したアプリケーションのパスワード，SQL 文の WHERE 句を用いてデータベースからログレコードを取得し Json 形式で送信する．

9. おわりに

本稿では，顔認識のためのプライバシー保護ツールキットの企画及び基本機能の開発を行った．個人情報の収集や利活用する Glassware や Web アプリケーションは，ツールキットを用いることで OECD8 原則を実現し，プライバシーを保護できる．現在，顔認識，ログを保存する度に被認識者に同意を求めているので，時間や場所などの状況毎に応答を自動化し，被認識者の負担軽減を図る．また，アプリケーション毎にログのアクセスを管理しているので，詳細にアクセス権限を設定し，適切な利用制限の実現を図る．

参考文献

[1] 米 Google、「Google Glass」で顔認識技術利用を当面禁止-INTERNET Watch, http://internet.watch.impress.co.jp/docs/news/20130603_601943.html
[2]グーグル・グラスの販売を中断、米グーグル写真 1 枚 国際ニュース：AFPBBNews, http://www.afpbb.com/articles/-/3036658
[3]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – OECD, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[4]不気味すぎる Google Glass アプリ「Name Tag」が公開 間近性犯罪履歴の閲覧も可能に: Google Glass info, http://googleglass.blog.jp/archives/3217987.html
[5]Emotient -Facial Expression Recognition Software,http://www.emotient.com/
[6]Autism Suite | BRAIN POWER, http://www.brain-power.com/autism/
[7]Dubai detectives to get Google Glass to fight crime, http://www.reuters.com/article/us-emirates-dubai-google-police-idUSKCN0HR0W320141002