特集号
招待論文

プライバシーに配慮したパーソナルデータ連携実現に向けたプロトコルデザイン
―OpenID Connect設計におけるプラクティス―

崎村 夏彦[†1]

[†1] (株) 野村総合研究所

新時代の経済を担う石油とも言われるパーソナルデータの流通であるが，あたかも石油が公害問題を克服せざるを得なかったように，プライバシー上の課題を克服しなければ大規模な実現は難しい．そのためには，プライバシー保護をプロトコルデザインの段階から埋め込むことが必要である一方，盛り込むべき項目は一般事業者が採用できるようなプラクティカルな配慮も不可欠である．本稿では，2014 年 2 月に標準として承認された OpenID Connect について，どのようなプライバシー保護手段が盛り込まれたか，それがどのようにプライバシー・トラストフレームワークの実現に寄与するかについて概観する．

1. はじめに

1.1 Privacy by Design と Privacy-First

世界経済会議（WEF）が2011年に発表したレポート「パーソナルデータ：あらたな資産カテゴリの出現（Personal Data: The Emergence of a New Asset Class）」[1]では，「パーソナルデータは新たな石油―21世紀の価値ある資源である」と指摘している．このパーソナルデータの利活用であるが，あたかも石油の利用が公害問題を生んだように，プライバシー侵害という外部性を必然的に生んでしまう．ある一定以上のレベルで石油を使うのには，公害問題を克服せざるを得なかったように，プライバシー上の課題を克服しなければパーソナルデータの大規模な利用も難しい．そのためには，パーソナルデータを取り扱うプロトコルにも，プライバシー強化の手段を設計の段階から埋め込むことが必要である．

一方，盛り込むべき項目は，一般事業者が採用できるようなプラクティカルな配慮も不可欠である．本稿では，2014年2月にOpenID Foundationにて国際標準として承認されたOpenID Connectについて，プライバシーへの配慮をプロトコル設計の段階からどのようにして組み込んだかを概観する．

2. パーソナルデータ連携と OpenID Connect

2.1 パーソナルデータとその連携

WEFの定義によると，パーソナルデータとは「人によって作られた，ないしは，人について作られたデジタルデータ」である．いわゆる個人データよりも広い概念であり，必ずしも個人の特定を必要としない．ISO/IEC 29100[2]でいうところのPersonally Identifiable Information（個人識別可能情報，PII）は「(a) その情報が関係する個人を特定することに利用可能か (b) 個人に直接・間接的に結びつけることが可能ないしはその可能性がある任意の情報」であるから，これに近い概念である．

上記のWEFのレポートでは，このパーソナルデータを (1) 自発的に提供されたデータ，(2) 観察されたデータ，(3) 推計されたデータ，の3つに分類している．自発的に提供されたデータというのは，本人が同意のもとに提供したデータである．Webサイトなどにユーザが入力するようなデータがこの代表例であろう．観察されたデータとは，ユーザのWebページアクセスの履歴や行動履歴などを観察することによって取得されるデータである．多くの広告ネットワーク（アドネットワーク．広告主から広告を一手に受注し，参画しているメディアへ広告を配信する）が利用しているのは，この類のデータ

ということになる．そして，最後の推計されたデータが，こうして集められたデータ等に何らかのモデルを適用して推計するもので，いわゆるプロファイリング（ユーザの行動他から，ユーザの持つ特性を推論すること）というのはこの範疇に入る．

このうち，あるWebサイトから別のサイトにユーザの同意と許可をもとにパーソナルデータを送信する「パーソナルデータ連携」が担当するのは（1）の自発的に提供されたデータで，OpenID Connectはこれを支援するものである．

2.2　OpenID Connectの概要

OpenID Connectを一言でいうと，パーソナルデータを本人の同意のもとに提供･管理するプロトコルである．数億ユーザを超えるようなきわめて大規模な実装を想定するとともに，プライバシーへの配慮を設計段階から組み込んでいるために，2014年2月26日に正式承認されたばかりのきわめて新しいプロトコルであるにもかかわらず各方面からの支持を受け，すでに各国で大規模な実運用に入っている．また，米国では，発行直後の3月13日に保健福祉省の公聴会で取り上げられ，次世代の医療情報連携システムのプロトコルとしての検討が同省の国家医療IT調整室（ONC）を中心に始まっている．

また，パーソナルデータの利用を本人の同意をもとに行うためには，まず同意をする本人を認証しなければならず，その認証結果も同意内容と同時に送ることになるため，単なる認証連携としても利用可能である．これを行うために，OpenID Connectでは以下の仕様を標準化している．

- OpenID Connect Core [3]
- OpenID Connect Discovery [4]
- OpenID Connect Dynamic Registration [5]
- OAuth 2.0 Multiple Response Type [6]

これらのうち，必須なのはOpenID Connect Coreのみであり，それ以外はオプションである．特徴として，APIのスタイルとしてはREST [7]，データ形式としてはJSONという，スケーラビリティに富んだ，最近の開発者の好みに沿ったプロトコルとなっている．当初はXMLを使うことも考慮されたが，開発者が集まるカンファレンスなどでアンケートをとったところ，XMLはやめてほしいという声が圧倒的であったために，JSONを採用することにした．また，通信はすべてHTTPSで暗号化することにして，開発者自身がアプリケーション層での暗号化は一般的なユースケースの場合考えなくてよいようにするなどの配慮も行った．

ただし，このようなモダンなスタイルをとるためには，元になるさまざまな部品を開発する必要があった．たとえば，SOAP/XMLであれば，署名にはXML Signatureを使うことができるわけだが，JSONに対する電子署名の形式は標準化されていなかったため，そこから標準化を始める必要があった．こうした「部品」に関しては，より広い範囲で活用可能な仕様として，OpenID Foundationではなく，IETF（Internet Engineering Task Force）に持ち込んで標準化を行っていった．こうして開発されていった「部品」には以下のようなものがある．

- RFC6749 OAuth 2.0 Framework [8]
- RFC6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage [9]
- JSON Web Token [10]
- JSON Web Signature [11]
- JSON Web Encryption [12]
- JSON Web Algorithms [13]
- JSON Web Key [14]

これらのうち，RFC番号のついていないものは，いずれもStandard TrackでWorking Group Last Callにはなっているものの，まだIETFでの標準化は終了していない．OpenID Connectは2013年2月段階のドラフトを参照するかたちで標準化を終えている．これは，以後テクニカルな変更はないことが見込まれたのと，「標準」として採用したいというプロジェクトがいくつも存在し，それ以上待つことは社会に対して害をなすと考えられたからである．

OpenID Connectのアクタには，以下の4つのタイプがある．

- 本人
- OP（OpenID Provider）：本人の認証を行い，データ提供の同意を取得し，データ・アクセスの権限管理を行う，いわば個人のエージェント．認証・認可を司るAuthorization Serverと，ユーザデータを提供するClaims ProviderとしてのUserinfo Endpointが存在する．
- RP（Relying Party）：OPよりパーソナルデータの提供を受ける．通常これをもとに本人にサービスを提供する．
- CP（Claims Provider）：個人の属性（Claims）を提供するサービス．OPが兼ねることも多いが，OPとは分かれて存在することも可能．

それぞれは複数存在することが可能で，それぞれの

RPは1つのOPに従属するわけではなく，個人も複数のOPを使い分けることもできるので，それぞれの関係は多対多である．この関係性を模式図にすると図1のようになる．ここで，本人は複数のOPに登録し，RPもまた複数のOPに登録している．

なお，これらのうち，OP，RP，CPは「トラストフレームワーク・プロバイダ」と呼ばれる事業体に登録されることが想定されている．トラストフレームワーク・プロバイダは，各エンティティの運営の適切性を担保するための仕組みで，各エンティティが守るべき運用基準を定め，その実施を管理する．

OP，RP，CPはそれぞれURLで表されるEndpointと呼ばれるAPIを1つ以上持っており，それらの間でデータがやりとりされる．そのCode Flowと呼ばれる場合の流れを表したのが図2のシーケンス図である．なお，UAはUser Agent，OP AuthZはOP Authorization Server，OP UserInfoはOP Userinfo Endpointの略である．

OpenID Connectは，ここで紹介しているCode Flowの他にも，Implicit Flow（認可コードの仲介なく，直接Tokenをブラウザに返す），Hybrid Flow（Code Flow, Implicit Flowを同時に実行する）の3種類を定義している．それぞれメリット・デメリットがあり，適切に使い分けることが期待されている．

次章以降では，このOpenID Connectの設計にあたって，プライバシーの尊重をどのように考慮していったかを説明する．

3. プライバシー検討の枠組み

3.1 プライバシー・フレームワーク

プライバシーを尊重してパーソナルデータの取得・利用・保持・開示をしようとした場合に，まず行わなければならないのが本人への影響を測ることである．それには，場当たり的な方策ではなく，包括的に考慮する枠組みが必要になる．それが「プライバシー・フレームワーク」と呼ばれるものである．

プライバシー・フレームワークは，言葉を定義し，アクタ間のやりとりを整理し，プライバシーを尊重するためにはどのような管理を行うべきか，どのような原則に従うべきなのかを整理したものである．OpenID Connectの設計に当たっても，こうしたプライバシー・フレームワークを元にして要件を引き出し，その実装を考える必要があった．当初はLINDDUN [15]と呼ばれるプライバシー脅威分析フレームワークの利用も検討した．しかし，同フレームワークには①同意のフレームワークがない，②図1からも見て取れるように，OpenID Connectのアクタ間の関係性はLINDDUN論文の中で例として挙げられていたものに比べて格段に多く，非常に煩雑になることが予想された．このため，実際には以下の2つを使って脅威パターンを出し，それに対してプロトコルとして何を対策として提供できるかを検討することとした．

- ISO/IEC 29100 Privacy Framework [2]
- RFC6973 Privacy Considerations for Internt Protocols [16]

3.2 ISO/IEC 29100 Privacy Framework

「ISO/IEC 29100 Privacy Framework」は2011年に制定された国際規格である．現在は無料でダウンロードできる

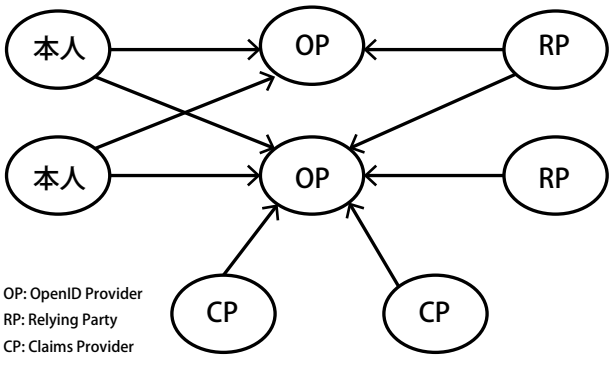

図1　OpenID Connect のアクタの登録関係性

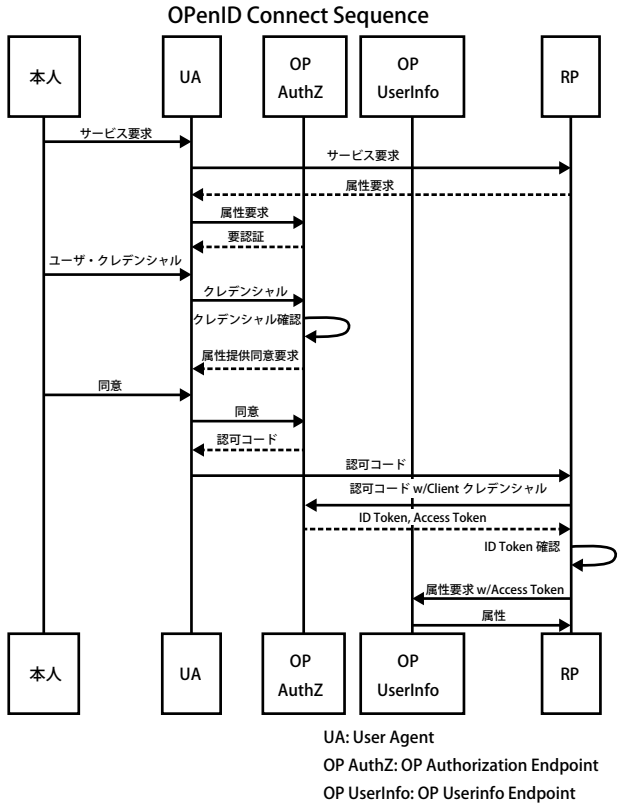

図2　OpenID Connect シーケンス

ようになっている．同規格は，PIIなどの言葉の定義を行い，アクタとして①本人②PII管理者③PII処理者④第三者を設定，その間の同意とデータ提供および処理の流れを定めている．OpenID Connectでいえばそれぞれ①本人②OP③Claims Provider④RPである．その上で，プライバシー保護要件を定め，プライバシーリスク管理を行うことを求めている．そして，これは①法規制要因②契約要因③業務要因④本人のプライバシー選好（特定の目的のためにパーソナルデータがどのように扱われるべきかについての本人の選択）などその他の要因の4つの要因によって影響されるとしている．個人情報保護法といった単一の法律よりも広い範囲の考慮を求めていることに注目すべきであろう．

加えて，ISO/IEC 29100はパーソナルデータの取り扱いに関して満たすべき①同意と選択②目的の正当性と規定③収集の制限④データ最小化（データの処理を必要最小限に抑えること）⑤利用，保持，開示の制限⑥正確性と品質⑦オープンさ，透明性，通知⑧個人の参加とアクセス⑨説明責任⑩情報セキュリティ⑪プライバシー法令の順守―の11の原則を挙げ，それらについて具体的に何をすべきなのかを，適度な粒度で記載している．

これらは，基本的に正当なデータ利用者が配慮すべき点に関して述べたものである．意図的な攻撃者に対するものも引き出せなくはないが，それには次に述べるRFC6973を用いたほうがよいと考えられた．

3.3 RFC6973 Privacy Considerations for Internet Protocols

ISO/IEC 29100は比較的使いやすい規格であるが，一般的なものであるので，インターネット上でのプロトコルの特性に鑑みた記載はない．これを補うのに使用したのがRFC6973である．これはInformationalなRFCではあるが，プライバシーに対する脅威と対策という形で書かれているので，インターネットプロトコルを設計する上では非常に使いやすい．

RFC6973では，脅威はセキュリティとプライバシー双方に関係する脅威と，プライバシーのみに当てはまる脅威に分けて，以下のように書かれている．

●セキュリティ・プライバシー脅威
- 監視・保存データの漏洩・侵入・誤帰属

●プライバシー特有のリスク
- 相関（複数の情報を同一の主体に属するとして結びつける行為）・特定（ある情報をある主体に結びつける行為）・2次利用・開示・除外（情報の存在や処理を情報主体に知らせないこと）

3.4 プライバシー・トラストフレームワーク

脅威に対する対策は，技術的対策と運用的対策が考えられる．すべてを技術的に解決しようとすることは費用対効果的に得策ではない．したがって，運用的対策としての「ルール」の設定は非常に重要である．プライバシー分野でいえば，JIS Q 15001が求めるような体系は典型的な「運用的対策」である．

一方，運用的対策を行おうとしたときに有用な技術的対策である「ツール」をあらかじめ用意しておけば，運用的対策の効果を高め，費用を引き下げる効果がある．

4. 考慮したプライバシー脅威と対策

4.1 OpenID Connect 設計にあたって考慮したプライバシーに対する脅威

OpenID Connectの設計にあたっては，上記2つの文書から以下のようなプライバシーに対する脅威を導き出した．

①-1 同意に基づかないデータの提供
①-2 選択肢のない場面での「同意」
①-3 条件反射による「同意」
①-4 同意の撤回機会の不提供
②-1 不当な目的
②-2 不十分な規定
②-3 錯誤を狙った規定
③-1 不必要なデータの収集
③-2 相関分析によるデータ生成
④-1 必要のないデータ・アクセス
④-2 Calling Home問題
⑤-1 目的外利用（二次利用）
⑤-2 不必要なデータ保持
⑤-3 同意を得た開示範囲外への開示
⑥-1 古いデータの利用
⑥-2 誤帰属
⑦-1 わかりにくいポリシー
⑦-2 ポリシーへのアクセスが難しい
⑦-3 通知なしでの変更
⑧-1 本人へのデータ開示の拒否
⑧-2 他人へのデータ開示
⑧-3 修正方法の不提示
⑧-4（開示時の）本人への過剰な金銭・時間負担
⑨-1 不十分な文書化と本人への伝達

⑨-2 保護レベルの不十分なRPへのデータ提供
⑩-1 監視・盗聴
⑩-2 サーバなりすまし
⑩-3 トークン偽造
⑩-4 トークン開示
⑩-5 RPによる要求の否認
⑪-1 プライバシー法令違反

4.2 実装した対策

これらの脅威に対しては，それぞれ以下のような対策を施した．方式の選択については，必ずしも技術のみにはよらず，場合によっては運用でカバーすることを考え，そのために必要な手段を用意した．また，OpenID Connectへの一般的な要件である，次の点にも配慮した．

(1) 基本形はきわめて簡単に実装できること．
(2) 非常に処理が高速で，スケーラビリティに優れていること
(3) モバイル・フレンドリであること．
(4) 開発しやすいように，JSON+RESTベースであること．
(5) ユーザマシンにインストールが不要であること

4.2.1 同意に基づかないデータの提供

OpenID Connectの枠組み内では，OPからトークンの発行を受けないでのデータ取得はできない．そのため，同意に基づかないデータ提供を防ぐためには，同意をする本人を適切に認証し，同意の取得をすれば良いことになる．仕様内では，前段の認証も，後段の同意（認可）も必須としている．ただし，後段の認可に関しては，明示的な同意ないしは「Conditions for Processing」に従った暗黙の同意の取得としている．この「Conditions for Processing」は，英国ico.（Information Commissioner's Office）がデータ保護ガイドライン[17]の中で処理の要件として規定しているものである．

4.2.2 選択肢のない場面での「同意」

同意が成立するには，それが自由意志に基づく選択の結果でなければならない．選択の余地のない条件のもとで取得した同意には有効性に疑義が残る．後続の処理に必須のデータは，その処理を要求しているのだからデータ提供が必要なのは当然だが，それ以外のデータに関しては必須ではないことが明確に示されるべきである．OpenID Connectでは，この目的のために，必須のものに対しては，属性要求時に「必須（essential）」という条件をつけて送ることができるようにして，必須と任意のものを峻別できるようにしている．

4.2.3 条件反射による「同意」

同意取得時の攻撃の主要なものに，鈍感化攻撃（desensitizing）とかクリック・トレーニングと呼ばれるものがある．これは，サービスを提供するにあたって毎回同意を求めるなど，過剰に同意を求めることによって，ユーザの同意ボタンを押すことへの警戒心をなくし，条件反射的に同意ボタンを押させるようにするものである．当初は無害なデータ要求を続け，条件反射になったところで，有害なデータ要求を行うことによって，有害なデータ提供に対してもデータ提供同意を得ることができる．

これを防ぐためには，明示的同意が必要な回数を減らすことが有効である．このため，当初のドラフトでは明示的同意を必ず取得することとしていたのを，「明示的同意ないしは処理の条件に合致すること」と変更した．

4.2.4 同意の撤回の機会の不提供

いったんデータ提供および利用に同意したとしても，その後のRPの動きを見ていて撤回したくなることは往々にある．OpenID Connectではこの目的のために，データ利用の有効期限をあらかじめ提示しておくとともに，任意の時点で，RPによるデータ・アクセスを遮断できるようにすべきとされている．具体的には，当該RPがデータ・アクセスのときに利用するAccess Tokenを無効にすることで実現する．この機能はオプションではあるが，Google（https://security.google.com/settings/security/permissions）に見られるようにすでに実装されている．

4.2.5 不当な目的

不当な目的のためのデータ要求を消費者が判別することはしばしば難しい．業務に対する知識がないからである．同様に，OPにとっても自動で認識することは難しい．

ある目的が正当かどうかは，最終的には業務知識に基づいて判断する必要がある．これを，データ要求者が行うと自分に都合よくするおそれがあるので，監督機関や消費者団体も含めたマルチステークホルダプロセスによって判断する必要があろう．

OpenID Connectでは，要求するデータの内容をファイルなどに記録しておいて，その場所を示すURLを送ることでデータを取得するモードがある．ある業務について正当と認定された要求のみを登録するレジストリを作り，このURLのみを使うことによって，不当な目的のデータ要求を排除することが可能になる．

4.2.6 不十分な規定

ISO/IEC 29100は，データ要求にあたって，要求者は，①必要な属性の指定，②取得目的の規定，③処理方式の

規定，④データの開示先（データにアクセスする自然人および開示先の法人）の規定，⑤データ保持期間および廃棄方法の規定を行うべきとしている．これらが規定されていない要求は不十分な規定しか持たないデータ要求といえる．これはシステム的にチェックするだけでなく，人の目も使って審査する必要があろう．

OpenID Connectでは，RPのクライアントをOPに登録するときに，プライバシーポリシーと利用規約のURLを指定することになっている．これらは人間が読んで理解できるデータを返さなければならない．前述の審査の仕組みで審査を通ったURIだけを登録できるようにすることによって，不十分な規定に基くデータ要求を排除することができる．

4.2.7　錯誤を狙った規定

この攻撃の典型例は，弊害の強い利用目的を，無害な多数の利用目的の中に隠すことである．これも，上記の審査プロセスであぶり出すことができる．問題が有る規定は登録を許さないようにすることによって，錯誤を狙った規定を排除することができる．

4.2.8　不必要なデータの収集

必要な属性を個別に指定するのではなく，属性をあらかじめ一定のバンドルにまとめておいてそれを要求する形式は，これまでのパーソナルデータ連携の中で広く利用されていた．しかし，これは必然的に過剰なデータの要求につながった．OpenID Connectは，こうした過剰なデータの収集を避けるために，個別属性ごとに指定してデータ取得要求を出すことができるようにしている．

4.2.9　相関分析によるデータ生成

本人の望まない相関分析には，少なくとも次の4つが考えられる．①異なるRPに対して提供されたデータを名寄せする．②同一のRPに対して異なるコンテキストで提供したもの（例，業務用と私用）を名寄せする．③異なる時点のデータ提供を名寄せする．④本人の属性や行動履歴と他人の属性や行動履歴との相関関係から本人の行動を予測する（いわゆるプロファイリング）．また，こうした名寄せが，本人の望まない「特定」につながって行く点も忘れてはならない．

こうした名寄せを防ぐには，①にはRPごとに別々のユーザ識別子を払い出すPPID（Pairwise Pseudonymous Identifier）方式，②には使用するアカウントのユーザによる選択，③にはEphemeral Identifierの利用が有効である．④は，プロトコルとしては範囲外だが，データの利用目的の明示と，望まないプロファイルが作成されたときの訂正手続きの際の本人認証手段としてのプロトコルが考えられる．

OpenID Connectの設計にあたっては，上記いずれの対策も実装可能にすることが求められた．PPIDの使用は，ユーザ指定識別子としてドメイン名だけを設定することにより可能で，個別に節を設けているし，ユーザによるアカウント選択は，別仕様であるAccount Chooser [18]という，ユーザがその時々によって使用するアカウントをGUI経由で選択できるようにした仕様と連携できるように設計している．③のEphemeral Identifierは，トランザクションごとに別のIDを降り出す方式で，PPIDをトランザクションにも拡張したものになる．

ただし，PPIDの実効性に疑問があることをここでは指摘したい．PPIDは，その性質上，ユーザ本人も覚えていることも口でいうこともできない．これは，RPにおける電話経由のユーザサポートを著しく困難にする．PPIDは，OpenID Connectの前のバージョンであるOpenID Authentication 2.0でも利用されていたが，この問題により，ほとんどのRPがその受入を拒否するか，メールアドレスや電話番号を必須にしてしまった．ほとんどのOPはRPごとの転送メールアドレスのようなものは用意していないため，実質的な名寄せIDとしてメールアドレスが使用可能になってしまい，PPIDの意味がなくなってしまった．

この経験から，OpenID Foundationでは，ユーザが複数の「アカウント」をOPに作り，それをコンテキストによってAccount Chooser経由で使い分けることを推奨している．

4.2.10　必要のないデータ・アクセス

OpenID Connectはデータ転送プロトコルであるから，RP内部に閉じたデータ・アクセスに関しては範囲外である．

OpenID Connectは，ユーザがオフラインのときのRPによるOPへのデータ・アクセスを可能にしている．このようなものを含んだUserInfoに対するすべてのアクセスログを，ユーザに提供するべきであるとしている．

4.2.11　Calling Home問題

酒屋で酒を買おうとしたとき，年齢確認のために免許証などの提示を求められることはしばしばある．このとき，免許証を提示しても，その事実が免許証の発行者に通知されることはない．

これが通知されてしまうような問題を，発行者（Home）に問い合わせ（Call）するということから，Calling Home問題という．たとえば，身分証明書に番号しか書いてなくて，その番号を使って身分証明書発行者に問い

合わせると年齢が得られるなどというのは，典型的なケースである．

OpenID Connectでは通常のケースでは，RPのデータ要求への同意をOPで行うために，いつ，誰に，ユーザがデータを提供しようとしているかが分かってしまう．このため，一種のCalling Home問題を抱えているといわれる．OpenID Connectの場合，OPはユーザの信頼できる代理人であるはず（そうでなければ，そこでデータの提供許可は出せない）で，これ自体に問題は少ないはずだが，特に欧州では指摘されることが多い．

この課題に応えるために，OpenID ConnectにはSelf-Issued Providerという，スマートフォンなどの上に個人専用に建てるOPの規格を作成した．これをたとえばプロキシとして利用することによって，いわゆるCalling Home問題は排除可能である．

4.2.12　目的外利用（2次利用）

RPによる悪意の目的外利用は，監査などで取り締まっていくしかないので，プロトコルの範囲外である．しかし，データに目的を結びつけておき，それと，データ利用者の目的が合致していることを審査してからアクセス許可を出すようにすれば，意図しない目的外利用はかなり減らすことができる．

OpenID Connectでは，データ提供時に，意図されたデータ提供先（aud）を指定することができる．この値はClient IDであり，policy_uriと結びついている．もちろん，policy_uriを明示的に返されるデータに入れておくこともできる．これらを活用することによって，不注意による目的外利用をかなり減らすことができると考えられる．

4.2.13　不必要なデータ保持

RPがデータを必要以上長い期間保持することは，データの漏洩リスクや，データの間の相関関係を不当に発見するリスクを増大させる．したがって，データの保持は最小限にするのが望ましい．そのためには，いつでも必要に応じてRPがデータを取得し直すことができるようにして，RPには短時間しかデータを貯めないようにするのが良い．

これを実現するために，OpenID Connectでは，データへのオフライン・アクセス機能（ユーザがオンラインでないときにも，ユーザデータをOPからRPが取得できるようにする機能）を提供している．また，データには「期限」の概念があり，これもデータ提供時に合わせて渡すことによって，RPにデータの期限内のみでの利用を要求している．

4.2.14　同意を得た開示範囲外への開示

ユーザから同意を得た範囲外への開示がプライバシーリスクであることはもはや説明の必要もないだろう．OpenID Connectでは，データの提供範囲をAudienceとして定義し，その識別子をデータ提供時のみに提供できるようになっている．

4.2.15　古いデータの利用

古いデータの利用は，不正確なデータの利用となり，それによって本人について間違った推計を行うリスクがある．また，古いデータと新しいデータを結びつけることで，本人が意図しないプロファイリングをしてしまう可能性もある．これらの理由により，古いデータの利用はさけるべきである．

OpenID Connectでは，前述のようにデータ利用期間を定めて渡すことができるので，このような脅威をある程度制御することができる．

4.2.16　誤帰属

誤帰属は，①不正確な認証，②不正確な相関分析（例：プロファイリング）などから生じる．対策としては，①必要十分な認証レベル，②本人によるモニタリングと訂正，などが考えられる．

対策として，OpenID Connectでは，「必要十分な認証レベル」をRPが要求できるように，認証レベル要求を認証時に出すことができるようにした．これはまた，RPにおける本人によるモニタリングと訂正に必要な認証レベルの提供にも成っている．

4.2.17　わかりにくいポリシー

ユーザは長文のポリシーは読まない．

これを利用して，その中にプライバシーインパクトの大きい事項を隠して形式的同意をとろうとする攻撃がある．

解決には，①ポリシーの重要事項をわかりやすく表示する標準的な方法の設定，②OPが不当なポリシーに対して警告を発する仕組みが必要．前者は，ユーザインタフェース規格であるので，OpenID Connect的には範囲外だが，②には寄与することができる．これは，policy_uriおよびrequest_uriの事前登録という形をとっている．

4.2.18　ポリシーへのアクセスが難しい

前述の通り，OpenID Connectでは，ポリシーの場所を指し示すpolicy_uriというパラメータを，RPの登録のときに設定できるようになっている．これが設定されている時は，OPはこれをユーザに示すことになっている．また，ユーザはいつでもこの情報にアクセスすることが可能である．

4.2.19　他人へのデータ開示

本人認証レベルが低い場合，本人へのデータ開示インタフェースから，なりすました他人がデータを取得してしまう可能性がある．どの程度ここを守るかは，開示するデータの性質による．リスクに応じた認証手段を使うべきであり，適切なレベルのものを要求できるように，OpenID Connectの要求パラメータにはAuthentication Class Reference (acr) が導入されている．ここで使う値はインターネットに関連する番号を管理する組織であるIANA (Internet Assigned Numbers Authority) のレジストリに登録することで拡張できる．デフォルトで提供されているのは，ISO/IEC 29115 Entity Authentication Assurance [19]で規定されているLevel 1 ～ 4である．

4.2.20　修正方法の不提示

データに間違いが見つかった場合の修正は，基本的にOpenID Connectのスコープ外である．ただし，修正方法自体はポリシーの中に記述するべきであろう．その意味で，登録時のポリシーの受け入れチェック項目に入れておくべきものである．

今後の展望としては，プライバシー強化の拡張仕様として，データ修正画面のURLを登録パラメータとして定義する等が考えられる．

4.2.21　保護レベルの不十分なRPへのデータ提供

ある一定の保護レベル（プライバシー原則の充足度）を上回る管理をしているRPを認定機関が認定して，そうしたRPのみをOPが登録を許すようにすれば満たすことができる．

5. 技術的プライバシー・トラストフレームワークの実現に向けて

上述の通り，多くの課題は「運用的」に対策されるものである．ただし，その「運用」の結果や状態を機械的に判別できることは，スケーラビリティの上からも重要であり，OpenID Connectはそのための多くの機構を備えていることがお分かりいただけたと思う．

こうした「運用」のカギとなるものとして，OpenID Conenctでは「トラストフレームワーク」を想定している．現在検討されている個人情報保護法の改正でも，マルチステークホルダプロセスによるトラストフレームワークの仕組みが検討されている．しかし，こうしたものがあっても，自動化を可能にする技術的な仕組みが伴っていないと要求されたスケーラビリティを満たせず，実効性を著しく減じてしまうことが想定される．OpenID Connectの設計は，技術的なプロトコルであるにもかかわらず，こうした制度的動向に特に注意を払った点が1つの特徴となっている．今後，他の分野のプロトコルを設計するときにも，こうしたプラクティスは参考になるであろう．また，プライバシーの強化という観点では，こうした技術的な基礎をもった制度を推進していくことが重要と考えられ，各国の制度設計においても，技術的プライバシー・トラストフレームワークの推進が待たれるところである．

参考文献

1) World Economic Forum: Personal Data: The Emergence of a New Asset Class, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (2014年7月1日現在).
2) ISO/IEC 29100 Privacy Framework, ISO/IEC (2011).
3) Sakimura, N., Bradley, J. and Jones, M.: OpenID Connect Core 1.0, OpenID Foundation (2014).
4) Sakimura, N., Bradley, J. and Jones, M.: OpenID Connect Discovery 1.0, OpenID Foundation (2014).
5) Sakimura, N., Bradley, J. and Jones, M.: OpenID Connect Dynamic Registration, OpenID Foundation (2014).
6) de Madeiros, B., Scurtescu, M., Tarjan, P. and Jones, M.: OAuth 2.0 Multiple Response Type Encoding Practices, OpenID Foundation (2014).
7) Fielding, R. and Taylor, R.: Principled Design of the Modern Web Architecture, ACM Transactions on Internet Technology (2002).
8) Hardt, D.: RFC6749 OAuth Framework 2.0, IETF (2012).
9) Jones, M. and Hardt, D.: RFC6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage, IETF (2012)
10) Jones, M., Bradley, J. and Sakimura, N.: JSON Web Token, http://tools.ietf.org/html/draft-ietf-oauth-json-web-token
11) Jones, M., Bradley, J. and Sakimura, N.: JSON Web Signature, http://tools.ietf.org/html/draft-ietf-jose-json-web-signature
12) Jones, M. and Hildenbrand, J.: JSON Web Encryption, http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption
13) Jones, M.: JSON Web Algorithms, http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms
14) Jones, M.: JSON Web Key, http://tools.ietf.org/html/draft-ietf-jose-json-web-key
15) Deng M., et al.: A privacy threat analysis framework: Supporting the Elicitation and Fulfillment of Privacy Requirements, Requirements Engineering, Vol.16, pp.3-32 (2011).
16) Cooper, A., Tschofenig, H., Aboba, B., et al.: RFC6973 Privacy Considerations for Internet Protocols (2013).
17) Information Commissioner's Office: Guide to Data Protection, http://ico.org.uk/for_organisations/data_protection/the_guide/
18) Brey, T., Sakimura, N. and Dingle, P.: Account Chooser.
19) ISO/IEC 29115 Entity Authentication Assurance (2012).

崎村夏彦（正会員）n-sakimura@nri.co.jp
（株）野村総合研究所上席研究員，情報処理学会規格調査会SC27/WG5小委員会主査，米OpenID Foundation理事長，米Kantara Initiative理事．主にDigital IdentityとPrivacy分野における国際標準化に従事．

採録決定：2014年12月1日
編集担当：青山幹雄（南山大学）