基般

パーソナルデータエコシステム構築に向けて
―自己情報コントロール権の実現―

佐古 和恵　NEC クラウドシステム研究所

パーソナルデータエコシステムとは

■基本的な発想

パーソナルデータがインターネットの新しい資源であるといわれて久しい．パーソナルデータを含むビッグデータを活用すれば，米国の医療分野で年間3,000 億ドル，欧州の自治体で 1,500 億ドルの削減ができるとしている 2011 年のマッキンゼーグローバルインスティテュートのレポートもある．

しかし，パーソナルデータは個人のプライバシーと密接に関係するため，現状では活用にあたってさまざまな制限がある．たとえば，日本では個人情報保護法ならびにその改訂方針が検討され，保護と活用を図るためのさまざまな義務が企業に課せられている．その背後には，生活者の不安の声も大きい．

一方で，海外に目を向けると，企業や組織がパーソナルデータを活用する観点ではなく，生活者が自分のデータを自分で活用する観点に期待が集まっている．自分の消費行動を俯瞰することによって，無駄遣いを防止する，地球にやさしい選択の可能性に気が付くなど，より適切な選択が可能になることが注目されている．さらには，本人にデータの利用目的と利用方法をはっきり伝え，場合によっては提供の対価を提示できれば，企業は本人の合意のもとで，自社が保持していない別の領域のデータを活用できる可能性がある．得られたパーソナルデータを活用して，企業がサービスを向上させたり，社会が改善したりすれば，結果的に生活者も恩恵を受ける．このような，パーソナルデータの「エコシステム」の検討が海外では始まっている．

■海外での取り組み

米国ではスマートディスクロージャ（賢い情報開示）政策として，政府の持つデータに関し，公開可能なものはオープンデータにして誰もが活用できるようにし，一方，パーソナルな情報で公開可能でないものは，本人が活用できるよう本人に提供する方針を宣言した．具体的には，退役軍人が自分の医療履歴をネットからダウンロードできるようにしたり，自分の健康状態をダウンロードできる Blue Button や電力消費をダウンロードできる Green Button 設置を推進したりした．

英国政府は midata プロジェクトとして，民間企業が持つ生活者に関するデータを本人に開示し，それらの情報がどのように活用できるかを研究した．これには，Google，ガス会社の British Gas，Lloyds TSB（銀行），通信業者の O2 といった民間企業が協力した．仏国では民間財団が Google，オランジュ，郵便貯金銀行，アクサなど 8 組織の協力の下で Mes Info プロジェクトを実施し，これには政府資金も投入された．

いずれも，パーソナルデータをどう活用するかは，企業が決めるものではなく，生活者に決定権があるものとした上で，パーソナルデータエコシステム（Personal Data Ecosystem：PDE）の樹立を目指している．すなわち，個人が収集したパーソナル

データを本人が活用するにとどまらず，適切な組織に提供することによって，企業や組織のサービスが改善され，それによってサービス享受者や環境にメリットが発生し，社会全体が恩恵を受けるエコシステムになるのである．**図 -1** にあるように，日本も企業が集めたパーソナルデータを企業がどう活用できるかの「企業軸」で考えるのではなく，データ主権者である個人がどのように活用できるか「個人軸」で考えるように変革すべきである．

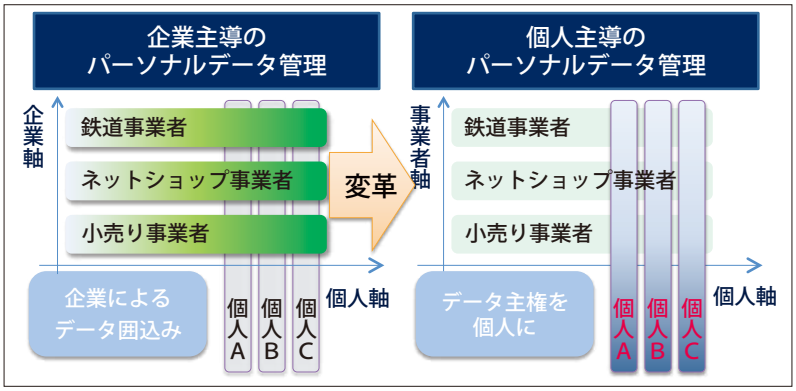


図 -1　個人主導のパーソナルデータ管理へ

パーソナルデータエコシステム（PDE）の設計

■ PDE のある生活

パーソナルデータエコシステムが確立した将来の生活を想像してみる．生活者 A さんは，自分専用の「パーソナル収納庫（Personal Data Store：PDS）」を持っている．鉄道会社の IC 乗車券を購入する際に，鉄道会社と契約し，利用履歴を自分の PDS に 1 日 1 回通知するような設定にしている．同様に，小売店や，ネットショップともそのような契約を締結する．いままで，紙で郵便受けに入っていた電気・水道・ガス料金もすべてここに入ってくる．月末に PDS の中を見ると，1 カ月分の自分の行程履歴，消費履歴を俯瞰することができる．これを用いて，会社の交通費清算や，家計簿管理が瞬時にできてしまう．年度末の確定申告の時期にブルーになることもない．

自分の車の走行履歴やメンテナンス履歴も自動的にこの PDS に登録されるようになっている．車を売却するときに，このデータをディーラーに見せれば，事故を隠ぺいしていないことの裏付けになるので，高く買ってもらえる．

医療機関に行くのも楽になった．先生に「熱が出たのはいつからですか？」と聞かれてもあわてることはない．これらの情報も PDS にある．お薬手帳の情報もあるから，以前どの薬で具合が悪くなったかが確実に分かって安心だ．

PDS に，友人からのメッセージが届いていた．PDS 間で直接メッセージをやり取りするので，途中で誰かに読まれる危険はない．友人曰く，B 会社のパーソナルトレーナーと契約したら，日々の運動量や食事内容から，適切なアドバイスがあり，みるみる体重が理想体重に近づいたそうだ．僕も一度診断してもらおう．

お気に入りのスポーツブランドから，先週購入した運動靴のアンケート依頼が届いている．歩数と感想を記入したら次回 500 円の割引クーポンがもらえるらしい．ちゃちゃっと記入しようかな．

いかがであろうか．一部のサービスは現在でも存在するかもしれない．しかし，データの入力の手間を最小限にし，異なる企業のさまざまなデータを横串にして提供されるサービスは，いまの個人の生活をもっと豊かにしてくれるだろう．いままで企業や組織が恩恵を受けていた ICT の力を，今後は生活者も活用できる．

■ プライバシーバイデザイン

PDE を構築するにあたって，プライバシー観点を組み込んだ設計，すなわち，「プライバシーバイデザイン」の考え方が重要になる．この概念は，カナダ・オンタリオ州の前プライバシーコミッショナーの Ann Cavoukian 博士が提唱したもので，**表 -1** に示すよう 7 つの原則からなる．

1. 反応ではなく事前対策を，対処ではなく予防を
2. プライバシーをデフォルト設定に
3. プライバシーを設計に埋め込む
4. 十分な機能性―ポジティブサム，not ゼロサム
5. 最初から最後までのセキュリティ―全ライフサイクルを通じた保護
6. 可視性と透明性―オープンにせよ
7. ユーザプライバシーの尊重―ユーザ中心とせよ

表 -1　プライバシーバイデザインの 7 原則

プライバシーに関する配慮は，設計後に追加するのではなく，設計当初から検討に含めるべきであるというのがこの概念の元にある考え方である．そして，仕組みとしてプライバシーが尊重されるようなシステム設計をしなくてはならない．たとえば，初期設定を変更しないまま使ってしまう人が多いことから，最初からプライバシー重視の設定をすべきである．ただし，プライバシーを重視したからといって，機能を劣化させることなく，機能とプライバシーを両立させなくてはならない．セキュリティは，始点から終点まで，さらに情報のライフサイクルのどの時点であっても，担保する必要がある．その上で，どうなっているか分かるように，状況を見える化し，透明性を確保するために，情報を公開することが重要である．最後に，一番重要なことは，ユーザを中心におき，ユーザのプライバシーを尊重する開発設計をすることである，と謳っている[1), 3)]．

■ PDE の構成

本節ではプライバシーバイデザインの原則を踏まえ，PDE を実現する主な 3 つの構成要素と，配慮すべき項目について述べる．3 つの構成要素とは 1）パーソナル収納庫（PDS），2）解析サービス，3）データ共有基盤，である（**図 -2**）．

パーソナル収納庫（PDS）

パーソナル収納庫（PDS）はパーソナルデータボルト（Personal Data Vault）とも呼ばれ，個人のデータの安全な格納場所になる．PDS の役割は，

- ユーザのパーソナルデータを外から集めてくる（ユーザ本人によるアップロードも含む）
- ユーザにデータを俯瞰させ，データの更新，削除などの管理や，一部を 2）の解析サービスに提供し，自分自身の生活支援に活用する．
- 友人や，パーソナルデータを活用したい他の組織に，自分のパーソナルデータを提供する．その際，提供時の利用条件を相手と交渉可能．条件の中には，利用目的以外にも，匿名化方法や消去日などが含まれる．あるいは，データそのものを提供するのではなく，データへのアクセス権だけを渡すこともできる．さらには，データ提供への対価も交渉することができる．

解析サービス

データを俯瞰して，人間がデータ間の因果関係に気が付く場合もあるが，PDS に格納される情報が大量になると，人手による解析も限界がある．PDS に集まったデータを解析して，最適な来月の携帯電話通話プランをすすめたり，引っ越し時の手続きを明確化したりするなど，本人の意思決定や活動のプロセスを手助けする本人専用のコンシェルジュのような解析サービスが PDE の重要な要素になる．Ctrl-Shift 社によると，このようなパーソナル情報管理サービス（Personal Information Management

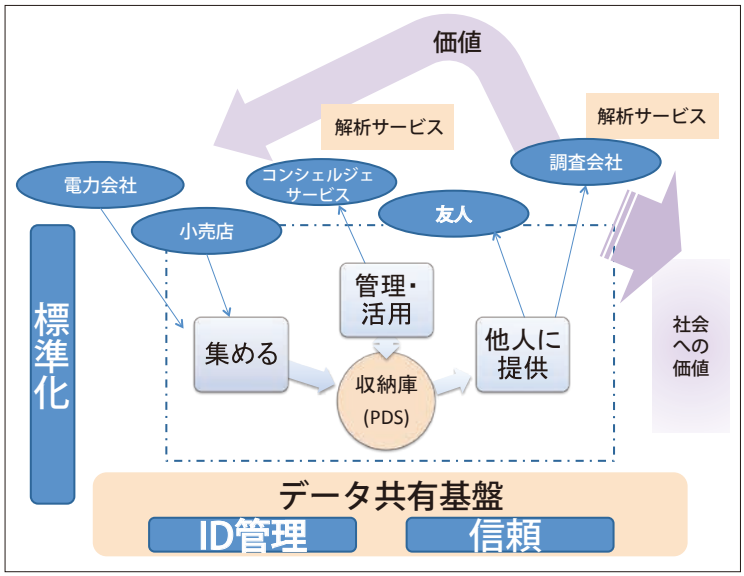


図 -2　PDE パーソナルデータエコシステム

Service：PIMS）の市場規模はイギリスだけで年間165億ポンド（約3兆円）もあると見積もられている．

解析サービスは，直接本人に価値を提供するだけでなく，パーソナルデータを活用して企業や社会のサービス向上に寄与させ，系全体に価値を与える役目も担う．

データ共有基盤

PDEがエコシステムとして機能するためには，データフォーマットを始めとする手順が標準化され，エコシステム内でのセマンティクスが統一されている必要がある．DropboxやiCloudを始めとする既存のPDSは，運営会社が独自に規格を作り，それぞれ異なるデータフォーマットで運用されている．これでは共有が難しい．

さらには，エコシステムの中でひとつひとつの格納庫が識別子を持ち，相互接続できるとともに，相互に信頼関係を持った空間になる必要がある．格納庫を中心にしたデータエコシステムがうまくまわるためのデータ共有基盤には，ステークホルダ間のルール作りが肝要である．

配慮すべき項目

PDEは，ユーザの自己情報コントロール権を発揮できる構造を目指しているが，適切に設計しなければ，PDS自身がプライバシーリスクになりかねない．PDS内のデータ保全はもとより，PDS内のデータやアクセス状況を，PDSの（本人以外の）管理者からも秘匿できるようにすることが重要である．

また，誰にどのデータをどの条件で開示するかを決めるのは，人間であるところのユーザである．人間が分かりやすいように，利用目的を表現したり，相互に誤解のないように条件を記述したりする標準的な手法が必要になる．さらに，ユーザの負担を軽減するために，ある程度，機械が自律的に処理可能な方向も目指すべきである．

安心・安全なPDEをプライバシーバイデザインの方針にのっとって具体的に構築しているスタートアップ企業に，Respect Network社がある．次章では，彼らの提唱するRespect Network構想を紹介する．

Respect Network構想

Respect Network構想とは，欧州アイデンティティ会議でプライバシー賞を受賞し，75を超える企業や組織が賛同している，PDEのための構想である．本構想は，主にPDSとデータ共有基盤の2要素を，技術，ルール作りとビジネスモデルの3つを調和させて具体化している．

■パーソナルクラウドとデータ形式

本構想の中核をなす発想は「パーソナルクラウド」である．企業が「クラウド」でパーソナルデータを収集・管理しているのと同様に，個人側も「クラウド」を持つべきという観点から，PDSを特にパーソナルクラウドと呼び，この中のデータは本人が全部のコントロールを持つように設計している．誰にどういう条件で見せるか，いつ消すかなど，すべて本人が決定することが前提である．

パーソナルクラウドがあることによって，変わってくる例として，サービス規約の管理方法が挙げられる．通常，サービスに加入する際に，サービス規約を表示され，ユーザは同意を求められる．同意しなければ，サービスを受けられないので，ユーザはサービス規約をよく読まずに同意ボタンを押すことが多いであろう．さらには，同意されたサービス規約に変更があっても，企業は再確認の義務はなく，ユーザが知らない間に新しい規約が有効になっている場合がある．パーソナルクラウドがあれば，サービス加入時にサービス提供者とパーソナルクラウドが契約条件を交渉できる．合意が成立した利用規約を双方が保管し，一方が規約を変更したい場合には，パーソナルクラウドとサービス提供者の間で再度交渉する．いままでのブラウザベースのWeb上の契約では実現されていないふつうの契約手続きが，パーソナルクラウドがあることによって，実現できるのである．

Respect Network構想では，サービス提供者な

ど，企業がパーソナルクラウドと対話する手段として，ビジネスクラウドがあるとしている．本構想では，クラウド対クラウドのプロトコルはオープンスタンダードであるべきと主張し，具体的には現在 OASIS で議論中の XDI（Extensible Data Interchange）技術を採用する．これはパーソナルクラウドの構造をセマンティックグラフとして定義した上で，セマンティックデータの交換プロトコルを規定している．さらにはパーソナルクラウド内のデータのアクセス権まで表現できる．すなわち XDI 技術の特徴的な点は「データ構造をグラフで表現する」ことと「データはアクセスポリシーと一緒に流通する」ということである．

■トラストフレームワークとレピュテーション

データエコシステムに必要な要件を，技術だけで成立させるのは難しい．たとえば，技術的に拘束できる形での利用目的や利用条件しか許されないとしたら，現状の技術では使い勝手の悪いものになりかねない．

一方で，技術的な拘束力がない場合には，相手が本当に合意したポリシーに従って処理するかどうかの保証は難しい．そこで，本構想では，参加者全員があらかじめ定められている「Respect Network トラストフレームワーク」を誓約することをルールとしている．さらに，その誓約を順守していることを他のメンバが評価するレピュテーション機能を有している．

Respect Network トラストフレームワークは，下記の 5 つの P を順守することを求めている．

- Promise「互いのディジタル境界を尊重する」
- Permission「誠意をもって，お互いと交渉する」
- Protection「信託されたデータやアイデンティティを保護する」
- Portability「会員の移動の自由をサポートする」
- Proof「すべての会員の利益のために合理的な範囲内で協力する」

レピュテーション機能は空間内のソーシャルな交流を活発にする目的にも存在する．空間内で活動が好ましい人や組織には他のメンバがプラスのレピュテーションスコアを与えることができる．

■ビジネスモデル

現在のネット上のサービスの多くは広告モデルである．すなわち，ユーザが無料で受けるサービスの運営コストは，ユーザに提示する広告料でまかなわれている．しかしこのモデルでは，ユーザ属性に関する情報が多いほどより高い広告収入が得られる側面があるため，ユーザの属性を多く集めようというインセンティブが働いてしまう．そこで本構想では，広告モデルを脱却し，「クレジットカードモデル」をビジネスモデルとして採用し，永続的にパーソナルデータエコシステムが存続することを目指している．

クレジットカードモデルでは，ユーザが年会費を支払い，カード加盟店のサービスを受ける．カード加盟店は一定の規約を守っている企業ということで，ユーザに安心感を提供する．一方で，企業もユーザにリーチするため，加盟費を支払ってでも加入するインセンティブが発生する．

Respect Network 構想では，ユーザや企業は会費を払って，Respect Network 空間上のクラウド ID を得る．このクラウド ID で，ユーザは加入企業のサービスを受けたり，企業はユーザの許可のもと，ユーザにリーチしたりすることができる．

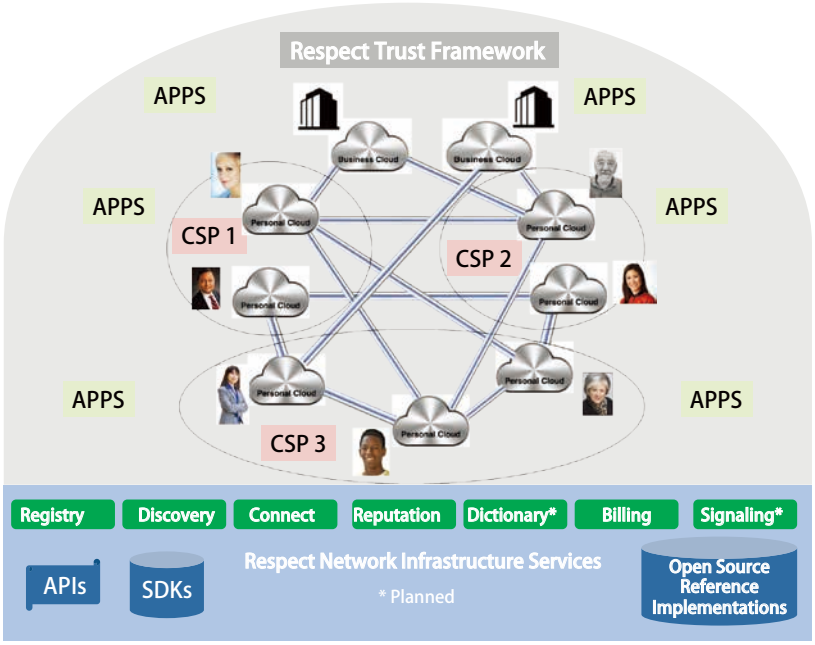
一方で現行のクレジットカード会社は，加盟店からトランザクションフィー（取引手数料）をもらって，場の運営をしている．Respect Network 社は，取引ごとのトランザクションフィーではなく，ユーザが企業のサービスに登録した際に，企業からリレーションシップフィー（関係性成立料）をもらうことを想定している．これは，ユーザから信頼を得て，ユーザとの関係性を築けることが企業にとっての価値だとしているからである．

■クラウドサービスプロバイダと基盤サービス

パーソナルクラウドは，ユーザ個人のポリシーが反映されるクラウドシステムという発想で設計され

ているが，すべての生活者が自分でシステムを管理できるとは限らない．そこで，クラウドサービスプロバイダ（CSP）という役割が登場する．インターネットに接続する際に，インターネットプロバイダと契約するように，自分のクラウドを代行管理してもらうために，Respect Network 空間内の CSP と契約する．

なお，CSP のユーザが不当にロックイン（囲い込み）されないために，ここでもプライバシーバイデザインの仕組みがある．具体的には，ポータビリティの原則に基づき，ユーザがどの CSP と契約しようとも，必要に応じて別の CSP に変更できる権利を認めているのである．そのとき，自分が貯めていたすべてのデータをそのまま移行できる．



出典）https://www.respectnetwork.com（2014.8.31 参照）

図 -3　Respect Network 構想

Respect Network 構想を打ち出した Respect Network 社の役割は限定的で，上記，パーソナルクラウドのネットワークの基盤サービスのみを提供する．具体的には，

- クラウド ID の管理（新規登録，ディスカバリーサービス，評判管理，課金）
- ユーザと企業，あるいはユーザとユーザを結び付けるコネクトサービス
- 空間内で同じセマンティクスが使える辞書サービス

が主なものである（**図 -3**）．

Respect Network 空間内では，上記基盤サービスを活用して，CSP やアプリケーション開発者をはじめとしたさまざまな企業が，ユーザをリスペクトした安全安心なサービスを提供するエコシステムを構成する．

■ VRM とパスワード問題解決

プライバシーバイデザインの原則にのっとり，ユーザ中心に設計した結果，パーソナルクラウドとビジネスクラウドが対等に関係性を築く環境が整うことになった．従来は，企業が顧客を管理する CRM（Customer Relationship Management）の観点が中心であったが，今後は生活者が企業を管理する VRM（Vendor Relationship Management）の観点が重要になってくる．

CRM の環境では，企業がユーザに ID をふるため，ユーザは企業ごとに ID とパスワードを管理しなければいけなかった．異なる複数の複雑なパスワードを管理することの困難性から，この仕組みは，パスワードの使いまわしを誘引し，ひいてはインターネット全体の安全性を低下させていた．VRM の観点を追求する Respect Network 構想では，自分のパーソナルクラウドにログインするためのパスワードを管理するだけでよい．企業からの認証は，公開鍵暗号技術を用いたクラウド認証が利用できるため，パスワードを使う方式に比べて，より安全なインターネット空間が実現できる．

国内での取り組み

国内でも，PDE 実現に向けた取り組みがいくつか立ち上がっている．本章ではそのうちの 2 つを紹介する．いずれも 2014 年度に発足したもので，現在，

さまざまな可能性を探っている途中である．

■ インフォメーションバンクコンソーシアム

慶大の砂原秀樹先生，東大の柴崎亮介先生を中心に，標記コンソーシアムが形成されている．インフォメーションバンク（情報銀行）は，生活者からパーソナルデータを信託されて，それを企業に提供するなどして運用し，その運用益を生活者に利子の形で還元するものである．また，通帳のように，自分の情報がどのように活用されているかを可視化する試みも行われている．

■ 集めないビッグデータコンソーシアム

これと連携して，東大の橋田浩一先生，須藤修先生を中心に「集めないビッグデータ」コンソーシアムも設立された．これは企業が全ユーザのデータを集めて活用するのではなく，個々のユーザが自分の情報だけをPDS（パーソナルライフレポジトリ：PLR）で管理し，必要に応じて企業がそのデータをもらい受けに行く，という発想である．その結果，企業にデータが集中するのではなく，個々のユーザの収納庫に分散管理されることになる．実際，企業が持っているビッグデータのうち活用されているのは5%に過ぎないことから，リスクを冒して100%のデータを集める管理コストを考えると，分散管理の方が合理的になるという主張である．また，本人にさえなかなか開示されないことがある企業内・組織内のパーソナルデータを，本人がコントロールすることによって，本人が許可した人には開示できるようにしたい，という思いもある．

安全安心なインターネット社会に向けて

現在のインターネットは，企業がブラウザ上から生活者に関するあらゆる情報を獲得して広告ターゲティングに活用したり，裏でデータブローカに販売したりしている．その分，ユーザは無料のサービスを享受できるが，自分の意思でその選択ができているとは言いがたい．また，企業の都合で，多数のパスワードを管理させられた結果，管理しきれなくなったパスワードでID盗難など，ネット上の安全性を脅かす脅威が深刻になってきた．World Economic Forumのレポート[2]にある通り，パーソナルデータを活用した今後の繁栄のためには，官民学が力を合わせて，生活者視点に舵を切る必要があると思われる．

本稿では，具体的なPDEの構想例を紹介した．これは，Respect Network社というスタートアップ企業による最初の一歩であり，今後どのように発展するか予断を許さない．しかし，これまでWebブラウザの機能制約によって企業に対して受け身だった生活者が「パーソナルクラウド」という強力な仕組みを活用することで企業と対等の立場で情報をやり取りできる世界を描いている．その世界では，暗号プロトコルをふんだんに活用し，さらなるプライバシーを尊重した機能の実現も可能になる．安全・安心，効率的で公平な社会実現のための壮大な試みであることは明らかであろう．

参考文献

1) Big Privacy: Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design, http://www.privacybydesign.ca/index.php/paper/big-privacy/
［日本語訳］ビッグプライバシー：プライバシー・バイ・デザインの適用によるビッグデータとパーソナル・データ・エコシステムの架け橋，http://www.privacybydesign.ca/content/uploads/2013/12/Big_Privacy-JP-0519.pdf
2) World Economic Forum Report : Rethinking Personal Data : A New Lens for Strengthening Trust, http://reports.weforum.org/rethinking-personal-data/
3) Personal Data Ecosystem (PDE) - A Privacy by Design Approach to an Individual's Pursuit of Radical Control. Digital Enlightenment Yearbook (2013). http://www.ipc.on.ca/images/Resources/digital-enlightenment-yearbook2013.pdf

(2014年9月8日受付)

■ **佐古 和恵（正会員）** k-sako@ab.jp.nec.com
NECクラウドシステム研究所技術主幹．Respect Network Security Architect．暗号プロトコル研究を経て，プライバシー研究に従事．