SNSにおけるプライバシー保護技術の現状

金森 祥子† 川口 嘉奈子‡ 田中 秀磨§

†情報通信研究機構 〒184-8795 東京都小金井市貫井北町 4-2-1
kanamori@nict.go.jp

‡千葉大学 〒263-8522 千葉県千葉市稲毛区弥生町 1-33
kanakothird@hotmail.com

§防衛大学校 〒239-8686 神奈川県横須賀市走水 1-10-20
hidema@nda.ac.jp

あらまし 近年、ソーシャルネットワーキングサービス（SNS）は、人間関係構築のための便利なツールとして利用されている。しかし、SNSにおけるユーザのデータ公開欲求と、技術や運用によるデータ保護には相反する点があり、結果として不適切データの流出による深刻なプライバシー侵害問題を引き起こす。本論文では、プライバシーを保護する概念であるプライバシー・バイ・デザイン（PbD）で言及されている「忘れられる権利」について注目し、SNSにおける能動的プライバシーと受動的プライバシーを検証する。また、「忘れられる権利」の実装要件を示し、既存技術の組合せにより実現可能な方法を提案し、プライバシーとセキュリティの観点から検証する。

A Privacy Preserving Scheme for Social Networking Services

Sachiko Kanamori† Kanako Kawaguchi‡ Hidema Tanaka§

†National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, JAPAN
kanamori@nict.go.jp

‡Chiba University
1-33 Yayoi-cho, Inage-ku, Chiba-shi, Chiba 263-8522, JAPAN
kanakothird@hotmail.com

§National Defense Academy of Japan
1-10-20, Hashirimizu, Yokosuka-shi, Kanagawa 239-8686, JAPAN
hidema@nda.ac.jp

Abstract It is a well-known fact that social networking services (SNSs) is mandatory to facilitate better personal relationships. However, such information on SNSs can lead to serious privacy invasion. In the Privacy by Design (PbD) concept, we especially focus on "the right to be forgotten." This paper shows requirements for implementing this right by examining active and passive privacy on SNSs. These requirements lead to technical solutions combining secret sharing and digital watermarking. We also evaluated our proposal from the standpoints of privacy and security.

1　はじめに

近年は、インターネットの普及発達に伴い、時間・場所を制約されることなく、あらゆる年代の人々が自らのパーソナルデータを発信できる状況にある。昨今のプライバシーを保護するための検討や対策は、誰でも自分のパーソナルデータを発信し、検索できるという状況も鑑みて実施される傾向にある。パーソナルデータに関するプライバシー保護の対策として、日本でも省庁による検討会が開催されており、総務省のパーソナルデータの利用･流通に関する検討会報告書 [1] では、基本理念としてプライバシー・バイ･デザイン (PbD)[2] が取り上げられている。

しかしながら、実際のソーシャル･ネットワーキング・サービス（SNS）は、これらの基本理念に則って運営されているわけではなく、一方、PbD もまた具体的に技術的解決策を提示しているわけではないので、さまざまな社会的問題が発生している。青少年が SNS にパーソナルデータをブロードキャストすることによる「リベンジ・ポルノ」や「デジタル・タトゥ」は、その一例として挙げられる。青少年は自分の将来に深慮せずに、コメントや写真を SNS に掲載してしまうことがある。この行動はまるで刺青のように、将来や過去の自分の名誉等、傷つける。一旦公開された情報は、削除できないことが多い。また、ストーカー（他者）によって、インターネット上にこの情報がばらまかれるケースも発生する。Google 社の会長 Eric Schmidt 氏は、2007 年に「過去をすべて消すことができるように、21 歳になったら改名できるという法律が必要である。」という将来を予見するコメントを残している [3]。この問題は、PbD の基本理念である、「最初から最後までのセキュリティ–すべてのライフサイクルを保護」を実現することにより解決する。また、この理念の実現のために、EU データ保護規則案では、「忘れられる権利」を規定している。このため、本論文では秘密分散と電子透かし技術を組み合わせて、「忘れられる権利」の実現を示す。SNS は、新たな人間関係を構築し、それを維持するために非常に便利で有益な手段ではあるが、プライバシーに関してはいくつかの問題が提起されている。本論文で提示する技術的解決策は、プライバシー情報が漏れることなく安全に SNS を使用する方法をユーザに提供する。

本論文の構成は以下のとおりである。まず最初に本論文で注目した「忘れられる権利」に関して論じる。この権利を実現するための要件を導出するため、第 3 節ではこの権利とプライバシーの関係を説明し、第 4 節でこの権利を実現するための要件を示す。次に、第 5 節では我々の提案する方法を提示し、第 6 節でこの方法をプライバシーとセキュリティの観点から評価する。この提案方法の適用と運用における問題点を第 7 節で検証し、第 8 節をむすびとする。

2　忘れられる権利

2012 年 1 月 25 日、欧州委員会から、「忘れられる権利」という条文を含む EU データ保護規則案が発表された [4]。「規則」は、EU 加盟国すべての国内法に優先し、「指令」より強い拘束力があるので、EU と商取引がある世界各国への影響が懸念されている。

「忘れられる権利」に関する EU における裁判事例を挙げると、スペインの男性が自分の過去の情報へのリンクを検索結果から削除するように Google に求めていた裁判で、2014 年 5 月 13 日、欧州司法裁判所は「検索エンジンプロバイダーは、一定の条件のもと、個人情報を含む Web ページへのリンクを検索結果から削除する義務がある」という「忘れられる権利」を支持する裁定を下した [5]。この裁定を受け、Google 社は、2014 年 5 月 30 日に削除要請窓口を設置している。

本裁判事例も示すとおり、EU における「忘れられる権利」は下記 3 ケースを含む [6]。

ケース 1 ：自分の投稿したパーソナルデータは自分で削除できる。

ケース 2 : 自分の投稿したパーソナルデータを、他人が拡散した場合、削除できる。

ケース 3 ：自分に関するパーソナルデータを他人が投稿した場合でも、削除できる。

本論文では、ケース 1 及びケース 2 について検討する [7,8]。

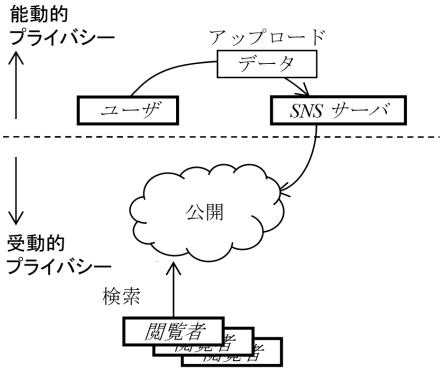

図 1: データ投稿フロー

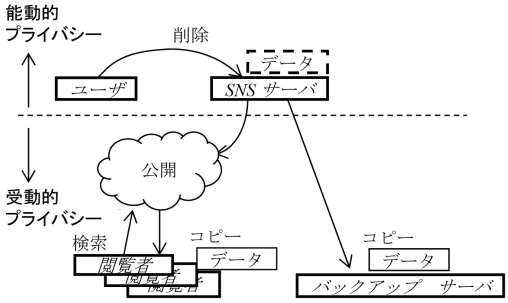

図 2: データ削除フロー

3 SNSにおけるプライバシーについて

3.1 能動的プライバシーと受動的プライバシー

プライバシーの定義は、とりまく環境や時代の変化に応じて変化しているが、プライバシーの性質の違いから、受動的プライバシーと能動的プライバシーに分ける考え方がある [9,10]。能動的プライバシーは、自己情報コントロール権 [11,12] であり、受動的プライバシーは、「放っておいてもらう」[13] ことである。

本節では、SNS におけるプライバシーに関して、ユーザの観点から論じる。ユーザは、データ投稿フロー（図 1）により、自分のパーソナルデータ（テキストまたは写真）を SNS にアップロードすることができる。同様に、データ削除フロー（図 2）により、自分のパーソナルデータを SNS から削除することができる。

自分のパーソナルデータを選択して投稿・削除できる、つまり自己コントロールできるので、能動的プライバシーの観点では、ユーザのプライバシーは保護されている。

受動的プライバシーについて検討するために、実社会に即して考えるとと、しつこくつきまとったり、覗き見をしたり、うわさをまき散らしたりすることが、他人の受動的プライバシー侵害となる。ネット上で考えると、必要以上に検索したり、他人のパーソナルデータをコピーして拡散したりすることが受動的プライバシー侵害となる。必要以上に検索することは、閲覧者の思いやりのある協力により回避できるが、全世界に閲覧者が拡がっている実情からすると不可能に近い。また、データ削除フローにおける「削除」は「永久にあらゆるところから削除」を意味しないことから、データのコピー・拡散を完全に阻止することもむづかしい。リベンジ・ポルノやディジタル・タトゥー等最近のプライバシー侵害事例では、過去は本人の意志とは関係なく再掲載されるという、SNS における未成熟な情報コントロールを提示している。よって、SNS ユーザは「忘れられる権利」を主張する必要がある。

多くの SNS サービスは、ユーザに対してプライバシー機能やプライバシーオプションを提供し、プライバシーを保護していると信じて疑わないが、この機能はあくまでもユーザの能動的プライバシーの一部を保護しているだけであり、受動的プライバシーは確保していない。プライバシーの観点では、能動的プライバシーと受動的プライバシーが両方同時に保護されていることにより、ユーザのプライバシーは完全に保護される。

3.2 忘れられる権利とプライバシー

現実の SNS において、忘れられる権利を実現するためには、次の 3 機能が求められる。

- 必要以上に検索されない
- 閲覧者は制限される
- 削除されたデータは再現されない

最初の要件は、閲覧者の協力が必要であるが、現実社会では実現することは少ない。SNS サービスはプライバシーオプションとして、2 番目の要件をユーザに提供しているが、データ投稿時だけであり、投稿後または検索時の受動的プライバシーは考慮されていない。能動的プライバシーだけではなく、受動的プライバシーに関しても忘れられる権利を実現するためには、ユーザからのデータ削除要求に応えることを、SNS プロバイダーに強制するだけでは不十分である。ユーザのプライバシーの両面、つまり能動的プライバシーと受動的プライバシーをの両方を達成するために、次節では忘れられる権利を実現するための SNS におけるプライバシーに対する 3 つの要件を提案する。

4 忘れられる権利の実現のための要件

忘れられる権利の実現のための要件を検討するにあたり、我々は SNS ユーザの受動的プライバシーに特化して検討した。SNS プロバイダーは、ユーザの能動的プライバシーを確立するための機能は提供しているが、受動的プライバシーについては認識をしていない。受動的プライバシーを保護するためには、検索条件を改良することと、削除されたデータの複製を防ぐという 2 つの方法がある。本節では、削除されたデータの複製を防ぐための 3 つの要件を提唱する。その要件とは、ユーザがサーバから自分のデータが削除されたことを確認できること、ユーザのデータが削除された後に、何者もデータを複製できないこと、ユーザがデータの削除を要請した後、他者がそのユーザのデータをコピーまたは保存して、再びインターネット上に掲載したとしても、ユーザは漏えいした情報の詳細フローをあばくことができることである。

4.1 データ削除の確認

ユーザが SNS から自分のデータの削除を依頼すると、サービスプロバイダはそのデータを削除する必要がある。しかし、現実の SNS では、データ削除を確認する機能がない。もし、SNS サーバのどこかにそのデータが残っているのではないかという疑いが生じたとしたら、ユーザの受動的プライバシー、つまり「放っておかれる権利」は満足されない。この透明性は、SNS ユーザの受動的プライバシーを保護するために必要である。

4.2 他者により複製できない状況

SNS に掲載された若い時の社会的に不適切な行為は、インターネット上に永久に残り、その人の将来にとって負の影響を及ぼす。しかし、本人が自分の情報を消したいか消したくないかに関わらず、既存のインターネットアーキテクチャは永久にその情報を保存する。

既存のサービスやシステムのプライバシーポリシーには、ユーザからデータ削除の要求があった場合には、そのデータを削除すると記載されているものもある。にもかかわらず、自分に不利なデータは何回も何回もコピーされる。自分の情報の削除を要求した場合には、何人もその情報を複製できないことは、忘れられる権利のための要件である。つまり、この要件が確立されてはじめて、ユーザからの削除要求は完成する。

4.3 データフローを特定する

自分のデータの削除要求に反して、他者がそのデータをコピーしたり保存したりすることがある。他者がそのデータを再掲載すると、ユーザのデータ削除は無効となる。他者がそのユーザのデータを掲載しても、ユーザがそのデータのフローを追跡できたり、誰がそのデータを掲載したかわかれば、この機能は他人のパーソナルデータ掲載の強力な抑止力となる。「データフローの特定」要件は、受動的プライバシー保護のために特に重要である。

他者が写真を SNS に掲載したあと、データ本来の持ち主（掲載写真の当事者）は自分のプライバシーが侵害されたことに始めて気が付く。リベンジポルノと言われる事例では、一人の女性が自分の顔写真と裸体が合成され他のサイトに

掲載されていることに気が付き、その削除のために脅迫メールにさらされることになった [14]。この事例は他者が写真を掲載したことによる、受動的プライバシーの侵害事例である。この理由により、データのコピーを防ぐための抑止力について検討した。この抑止力を要件として入れることにより、受動的プライバシーの侵害を防ぐことができる。

5　提案方法

5.1　提案方法の概要

我々の提案方法は既存の技術の組み合わせにより成り立っている。

- 秘密分散 [15]
- 電子透かし [16，17]

秘密分散には多様なより効果的な方法もあるが、今回は基本的な方法を用いて説明する。また、電子透かし技術は、多くのユーザが自分の写真を SNS に公開しているので、今回は画像データのための電子透かし技術を使用している。

我々の提案する手法は、オリジナルデータがテキストだけであったとしても、イメージデータに変更する必要があるので、効率と使いやすさに少々問題はある。この問題については, 第 7 節で述べる。我々の提案手法の構成要素は下記のとおりである。

・ ユーザ：サービスと契約し、コメントや写真を SNS に公開する。

・ サービス：SNS サービスプロバイダー

・ TTP：サービスと契約をしている信頼できる第三者機関

・ 閲覧者：SNS を検索し、ユーザのコメントを読む一般的なユーザ

・ 悪意ある閲覧者：ユーザのデータ P を故意に拡散する者

ユーザのデータ P は、ユーザが自分の忘れられる権利により他者に「忘れてほしい」データである。

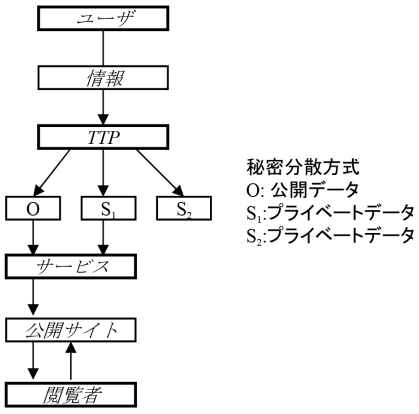

図 3: 公開データのデータフロー

5.2　プロトコル

我々の提案方法は、次の 3 つのプロトコルから構成される：登録フェーズ、利用フェーズ、取り下げフェーズ。

【登録フェーズ】

ステップ 1：ユーザはサービスにアカウントを作成する。サービスはユーザにプライバシーオプションと契約している TTP を提示する。

ステップ 2：ユーザはプライバシーオプションを設定し、サービスと TTP にその設定を提出する。TTP 経由ユーザとサービスを結ぶデータの流れが作成される。

「プライバシーオプション」とは、情報が公開される範囲を設定するだけであるということに注意する必要がある。例えば、タイトルのみ、タイトルと最初の一文だけ、写真以外はすべてなど、公開可能なデータを指定する。しかし、この公開データは、公開範囲が設定されただけで、「忘れられる権利」については言及されていない。さらに、プライバシーオプションは、いつでも変更することができるが、変更するたびにユーザはサービスと TTP に変更を届け出る必要がある。

【利用フェーズ】

ステップ 1：ユーザは自分のコンテンツを TTP 経由でサービスに送る。（TTP はプロキシサーバと同じ役割を役割を果たすので、ユーザは TTP を意識する必要はない。）

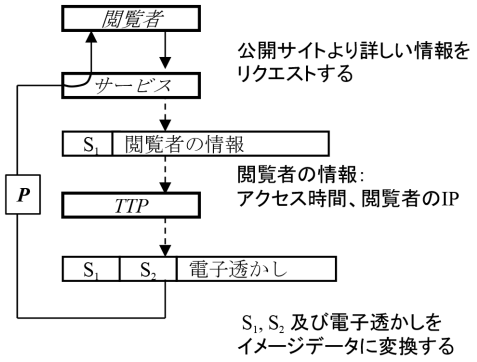

図 4: プライベートデータのデータフロー

ステップ２：TTP はユーザのプライバシーオプションに従って、ユーザのコンテンツを公開部分 *O* とプライベート部分に分割する。プライベート部分に関しては、秘密分散手法により、*S1* と *S2* を生成する。TTP は *O* と *S1* をサービスに送付する。

ステップ３：サービスは *O* を公開し、閲覧者は *O* だけを読むことができる。

ステップ４:閲覧者がさらにコンテンツを読みたい場合は、サービスにリクエストをする。サービスは閲覧者の情報とともに *S1* を TTP に送付する。閲覧者の情報としては、アクセス時間と閲覧者の IP アドレスが最低限必要となる。

ステップ５：TTP は *S1* と *S2* を用いてユーザのコンテンツを復元し、JPG や PDF ファイルなどのイメージデータに変換する。変換したイメージデータに対して、TTP は電子透かし情報を挿入する。送付されるデータには、最低限閲覧者のアクセス時間、閲覧者の IP アドレス及び TTP の署名が含まれる。*P* は最終的に生成されるイメージデータであり、TTP はサービスを経由して *P* を閲覧者に送付する。

ステップ６：閲覧者はイメージデータ *P* を受け取る（図４）。

【取り下げフェーズ】

ステップ１：ユーザは、SNS に掲載したデータの削除を TTP とサービスに要求する。

ステップ２:TTP とサービスは、削除要求をされたデータに関する *O*、*S1*、*S2* を削除する。実際には、秘密分散機能により、*S1* または *S2* のどちらかを削除するだけで十分である。

我々の提案手法は簡単で既存手法の組み合わせではあるが、プライバシーの観点から考察すると、忘れられる権利を実現するための要求は満たしている。

6　提案方法の評価

6.1　プライバシーの観点からの評価

プライバシーの観点から評価するために、能動的プライバシーと受動的プライバシー両方の実現を目指した。

秘密分散の設定により、ユーザは投稿データを読むことができる人を限定することができる。例えば、3 /3 秘密分散を利用すると、投稿データは３つのデータに分割される。つまり、*S1* はサービスへ、*S2* は TTP へ、*S3* はユーザに送付される。結果として、サービスが情報を公開するためには、ユーザの同意が必要となる。よって、我々の提案は、ユーザが自分のデータを完全に管理でき、能動的プライバシーを保護できる方法である。

一方、この手法では、受動的プライバシーも実現することができる。サービスを利用する際に、一般的な閲覧者は公開部分 *O* だけを読むことができる。しかし、プライベートデータは、TTP とユーザが閲覧者の情報を確認することにより、情報が公開される。よって、ユーザのコンテンツは、不必要な検索やビッグデータの自動生成から保護される。

6.2　セキュリティの観点からの評価

我々の提案において、２種類のインシデントが考えられる。

ケース１）契約している TTP 廃止または変更による情報漏えい。

ケース２）取り下げ後の情報拡散。

秘密分散手法はケース１の対応策となることは自明である。我々の提案では、サービスも TTP もデータのフルコンテンツを保持していない。もし秘密分散手法が安全であるならば、*S1*

または $S2$ のみでコンテンツを復元することは不可能である。よって、我々の提案手法はケース１に対して安全であることが導かれる。忘れられる権利を検討するにあたり、ケース２は解決が難しい。ケース１の分析より、サービスとTTP は取り下げコンテンツを拡散することはできない。よって、ケース２は、取り下げの前に作成されたイメージデータ P に基づく。この問題の解決方法として、２つの手法を利用する必要がある。

解決方法１）P を利用する際に時間制限を設ける。

解決方法２）利用フェーズのステップ５の電子透かし技術

我々は、5.2 節で時間制限については述べていない。しかし、最近のオンラインサービスでは一般的な技術であり、設定をすることは難しくはない。データに時間制限を設定することは、閲覧者によるデータのコピーや拡散の可能性を削減することになるので、インシデントの発生を防ぐ観点から、解決方法１は機能として設定されるべきである。一方、解決方法２は、インシデント後にその効果を発揮する。悪意ある閲覧者がユーザのデータ P を故意に拡散してしまった場合、我々は電子透かしによりその悪意ある閲覧者を追跡することができる。ユーザによるデータ取り下げ前でも、ユーザ本人が情報拡散を望んでいない場合は、拡散源を特定できる。解決方法２の欠点は、テキストデータの拡散に関しては効果がないことであるが、電子透かしはデータ処理に関して安全性が高いので、導入されるべきである。

7　提案方法の応用と実用

我々の提案手法は、プライバシー保護を実現するサービスへ応用できる。我々の提案手法の電子透かし機能は、情報の漏えい源を確定することができるので、PbD の「可視性と透明性–公開の維持–」にも適用することができる。電子透かし技術はユーザとプロバイダー双方に遡及効果のある削除の追跡を可能とする。秘密分散技術もユーザ、サービス、TTP がアクセスコントロールを調整することができる。機密性の高い情報を得るためには、閲覧者が共有するべき分割された情報の構成部分の数は増える。TTP が情報の分割回数を増やすことにより、さらに繊細なプライバシー情報にも対応できる。

一方、運用方法において、我々の提案手法にも問題はある。我々のプロトコルは、電子透かしを挿入するために、テキストデータをイメージデータに変化する必要がある。将来の研究課題として、我々はこのプロトコルを実装し、電子透かしを挿入する際の効率性と利便性について、検証する予定である。根本的な解決方法としては、インターネットアーキテクチャそのものに対する劇的な変更が必要である。サービスがプライバシーを保護する強固たる構造を確立するためには、法的なメカニズムも必要である。

8　むすび

SNS は人間関係構築のために、特に若い世代で広く利用されているが、これらのサービスに投稿されたコメントや写真はプライバシーを侵害する可能性を持つ。SNS のすべてのユーザは、PbD の理念を満たすサービスの提供を待ち望んでいる。この理念の中で、将来 SNS を安全に利用するために、我々は特に「最初から最後までのセキュリティ–すべてのライフサイクルを保護–」に焦点をあてた。この理念に対する具体的な解決方法を導くために、忘れられる権利の実現というステップを踏んだ。本論文では SNS における能動的プライバシーと受動的プライバシーに関して議論し、さらに忘れられる権利との関係についても検証した。その結果、忘れられる権利を実現するための３つの要件を導出し、これらの要件を実現するための技術的解決方法を提案し、その方法を評価した。本論文では、ユーザ（パーソナルデータ所有者）から見たセキュリティに関して評価したが、それぞれの立場により相反する、または矛盾する要件も発生する。その要件の最適なバランスをとるためには、技術的解決だけではなく、インターネットアーキテクチャと法的なメカニズムからのアプローチも必要となる。我々の提案手法が、将来

的に SNS の安全な利用とその重要な意義を継続して享受することに貢献することは明らかである。

謝辞

本論文作成にあたり、ご協力いただいた公益財団法人未来工学研究所笠井祥氏に感謝いたします。本研究は JSPS 科研費 25884009 及び科研費基盤 (C)24560791 の助成を受けたものです。

参考文献

[1] 「パーソナルデータの利用・流通に関する研究会報告書〜パーソナルデータの適正な利用・流通の促進に向けた方策〜」, 総務省, 2013 年 6 月 http://www.soumu.go.jp/main_content/000231357.pdf

[2] A. Cavoukian, "Privacy by Design," http://www.privacybydesign.ca/ (2014-04-10)

[3] J. Jarvis, "PDF: Eric Schmidt," Buzzmachine blog, http://buzzmachine.com/2007/05/18/pdg-eric-schmidt/ (2014-03-17)

[4] The EU Data Protection Reform 2012:Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design, Jan. 2012 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF (2014-07-25)

[5] EU 司法裁判所プレスリリース 2014 年 5 月 12 日 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (2014-07-11)

[6] J.Rosen, "The Right to Be Forgotten", Stanford Law Review, Online 88, 2012 年 2 月 http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten (2014-07-11)

[7] S.Kanamori,K.Kawaguchi,H.Tanaka, "Study on a Scheme for the Right to Be Forgotten",ISITA2014, 2014 年 10 月

[8] Reviewer's comment of [7]

[9] 青柳武彦, "情報化時代のプライバシー研究", NTT 出版, 2008 年 4 月

[10] 金森祥子, 川口嘉奈子, 田中秀磨, "個人情報と受動的プライバシーに関する一考察, The 30th Symposium on Cryptography and Information Security, 2C1-2, 2014.

[11] A. F. Westin, "Privacy and Freedom", New York: Atheneum, 1967.

[12] A. F. Westin, "The origins of modern claims to privacy", Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984.

[13] S. D. Warren and L. D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. IV, No.5, 1890.

[14] http://www.dailymail.co.uk/news/article-2581466/ (2014-03-26)

[15] A. Shamir, "How to share a secret," Communications of the ACM, Vol. 22, Issue 11, pp. 612-613, 1979.

[16] I.J.Cox, J.Kilian, F.T.Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, Vol.6, No.12, pp. 1673-1687, Dec.1997

[17] F. Harting, M. Kutter, "Multimedia watermarking techniques", Proceedings of the IEEE, Vol.87, No.7, pp. 107901107, Jul.1999