不正者追跡・排除可能な匿名認証ライブラリシステムの開発
～SENSU Project～

１．背景

近年、様々な場でプライバシ保護について叫ばれていますが、これを法的観点から考えるとどうなるでしょうか？我が国においては、憲法 13 条にある包括的基本権を根拠とする人権を構成する権利としてプライバシに関する権利は位置づけられています。また、2005 年 4 月に主として事業者を対象とした「個人情報の保護に関する法律」、いわゆる、個人情報保護法が施行されます。

個人情報保護法によると、個人情報の制御権はあくまでも情報の当事者本人に属するということになっています。これが適用されると、現状の情報の扱いが大幅に変わる可能性があります。わかりやすいところで考えますと、近年頻繁に発生した個人情報などの漏洩などの事件は損害賠償要求などの民事訴訟の対象となることも予想されます。特に、5000 人以上の個人情報を取得した事業者は取得情報の種類や方針が変わると、必ずその情報の当事者である個人に「どのような変化か」ということについて報告する義務を持ちます。つまり、履歴取得の方針変換のたびに、常に個人へ通知しなければならないのです。

顧客の情報は企業にとって非常に有益なものとなります。それらの情報を利用することによって、より消費者のニーズにあったサービスを提供することができます。一方で、大量の情報を保持し、運用していくことは社会的だけでなく法律的な観点からもかなりのリスクを伴うものであろうということは、容易に想像できます。

消費者動向の調査のための情報解析として、個人情報の利用は欠かすことはできませんが、個人情報をかかえることは漏洩の際のリスクも含め、コストのかかるものとなります。そこで個人情報を管理する手順・体制の確立が不可欠となるのです。

２．目的

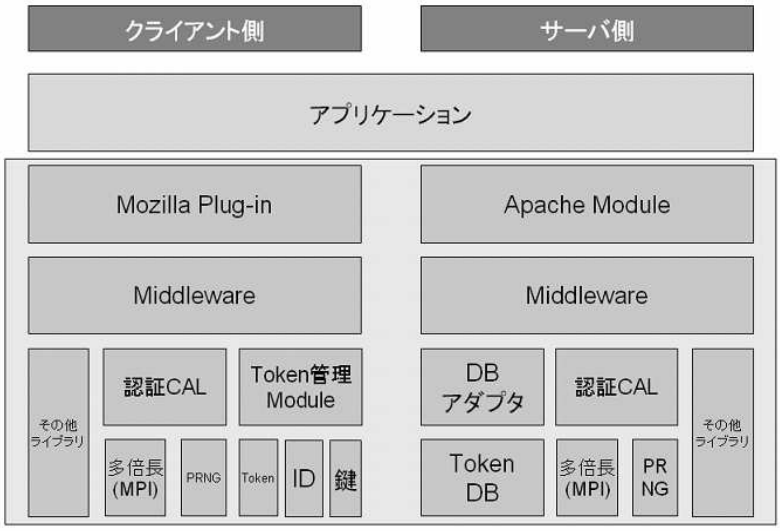
現在の消費者動向調査の基本的な発想は「誰が」「いつ」「何をやった」か、という情報を集めることだと思います。一見するとあたりまえのことですが、我々は実はこの時点で必要以上の情報を集めていると考えます。

また、新しい動向を調査するためには新しい情報の収集が必要です。しかし、現在の個人情報保護法の枠組みでは情報収集の方法は容易に変更できるものではありません。

そこで、我々は、新しい認証基盤の SENSU を提案します。従来の枠組みでは、消費者に対して行われた全てのサービス履歴を多少の差はありますが、基本的に一つのデータベースに保存する傾向にありました。しかしながら、誰がいつどこでどのように何をしたのか非常に個人の利用履歴に関する情報が全て一カ所に残り、この情報が漏洩した際の被害は計り知れないものと予想されます。これに対し、SENSU を利用すれば、ユーザ登録時の個人情報と利用履歴を完全に暗号によって切り離すこ

とが可能です。
我々はこれを「匿名性」によって実現している、と呼んでいます。既存の認証方法では、権利の確認を行うため、ユーザの名前を特定しサービスを行ってきました。また、その一方で権利の確認を行わずに誰でもサービスを受けられる、というサービスも存在しました。
これらに対し、SENSU はユーザがアイデンティティを見せなくても、権利の確認をすることができます。これにより、サービス提供者は、利用者が存在することは確認できますがその利用者が誰であるかということまでは特定できません。
従来の似たような方式では、権利の更新を行うことができるものはありませんでした。それらと比べると SENSU では権利の更新を行うことができるため、様々な用途に応用することができます。
匿名性を悪用した良識のないユーザをグループから排除することもできます。履歴情報においては、必要に応じて各情報をつけることによって、「個人情報保護法によって義務づけられているユーザへの通知」の必要のない情報収集も可能となります。権利の更新の際に、権利の種類を変更することも可能となっています。
この権利はもちろん偽造ができないようになっていますし、もし、電子情報の不正なコピーによる二重使用が行われた場合には、ユーザを特定することもできます。

３．開発の内容
SENSUはC言語で実装されており、フリーなライブラリとして公開されています。また、ソースコードも公開しているため、内部での動作を検証することができます。
SENSUは認証計算APIや各種情報の管理APIといった基本的なAPIから構成されるライブラリの他、ライブラリを簡便に扱うためのWrapper APIも提供しております。
またアプリケーションの構築を容易にするためのウェブサーバのモジュールやブラウザのプラグインの公開も予定しています。



４．従来の技術との相違
我々が作成した物は、情報収集などのアプリケーションにおいて、個人を特定することのできる個人情報と利用履歴を切り離すことの可能な新しい認証の実装である SENSU です。
また、この新しい認証基盤は Anonymous Token Scheme という暗号プロトコルを元にした新たな認証方式であり、我々の言うところの「匿名性」をもったもので、非常に高い汎用性を備えています。
また、実装上起こりうるであろうセキュリティホールをできる限り減らすために、IPA CRYPTOREC などの暗号評価団体による評価基準を元に、SENSU 内で利用される暗号はすべて先に述べた暗号評価において安全である、と評価されたものを利用しています。この SENSU システムはフリーなソフトウェアであり、自由に利用することができます。
同時に、暗号が元ということで、鍵の作成など利用者にとって馴染みの薄い動作に関しては、ユーザビリティも考慮し、自動で行うための機能も備えております。これにより、より高い普及を実現することができると考えています。

５．期待される効果
最近の匿名性のイメージというと、サービス提供者が不特定多数に対してサービス提供を行い、ユーザの情報をはじめから認証を行わない、ということによってサービスを行っているサービスを指している傾向がありました。しかし、実際にはサービス提供者はユーザが本来そのサービスを受けるべき人であるかどうか(たとえば、お金を払った、その会員であるなどなど)であることを認証できるべきでありますし、かつ、何か問題が起きた場合は起こした人を排除したい、もしくはよい行いを行った人はよりそのサービスに対して貢献をしてほしい、ということは非常にわかりやすい発想です。本プロジェクトでは、現状のインターネット利用者にたった、ライブラリを作成することによって、より、利用者を増やし、普及を促すことができると考えます。特に現状では、2ch や Slashdot に代表される BBS において、荒らし対策が急務となっています。Slashdot では、独自のモデレーションによって対策を行いより質の高い情報配信サービスとして評価が高かったが、同一人物による短期間の複数書き込みによる問題が起こっています。このような現状から判断し、本プロジェクトのライブラリは非常に必要性の高いものと考えています。また、同時に従来では実現できなかったアンケートでの二重投稿を防ぎかつ、ユーザの匿名性を保つことなども実現できます。これにより、先日問題になったプロ野球のオールスターでの心ない投稿による上位への選出などもなくなると考えます。

６．普及の見通し
この SENSU は、匿名認証のフリーな実装として公開しております。これは、普及においては欠かすことのできない要素の一つであろうと考えています。また、来年の

プログラミングシンポジウムにおいての実用も決まっており、非常に注目が高いものとなっております。

７．開発者名

- 繁富利恵(東京大学情報理工学研究科 sigetomi@imailab.iis.u-tokyo.ac.jp)
- 副田俊介(東京大学総合文化研究科 shnsk@graco.c.u-tokyo.ac.jp)