プライバシ保護の一手法の提案

京都情報大学院大学
神垣　智一　廣瀬　誠
山下　泰芳　高　弘昇
宮本　慎　内藤　昭三

NTTアドバンステクノロジ株式会社
中口　孝雄

京都コンピュータ学院
饗場　繁
藤田　和也

近年，個人情報保護に関して様々な議論が行われている。その背景としてはInternetビジネスの急速な発展が影響している。なぜならば，Internet上でのビジネスでは何か物を一つ買うといったことでも，ある程度の個人情報が必要となってくる。例えば配送先の住所，決済に使用するクレジットカードの情報といったものである。Webサイトを運営している企業はこれらの情報を蓄積し，マーケティングなどを行い，新たなビジネスを展開している。またユーザはよく利用するサイトに自分の個人情報を登録しておき，ID･パスワードを用いるなどの認証技術で本人確認を行い，蓄積されているDatabaseより個人情報を引き出し，入力の手間を省くといったことに利用している。しかしながら，現在この一連の流れに問題が生じてきている。それは，これらの情報を1社で管理するには多大なコスト，個人情報漏洩リスクが非常に高いという問題である。また利用者は，なによりも個人情報流出における個人のプライバシ侵害に問題を感じている。しかしながら購入者や利用者の情報を取得しなければ今後のビジネスに生かすことができなくなり，Internet上でビジネスを行うメリットがなくなってしまうのも事実である。そこで我々は1社で管理するのではなく，数社により1つの個人情報を管理することで個人情報漏洩の危険性を少なくし，またプライバシ保護の観点からも非常に優れた方式を提案する。

1. 現在のプライバシ保護の問題点

eビジネスにおけるプライバシ保護はeビジネスを執り行う企業にとって非常に重要な業務の1つとなっている。しかしながら現状では様々な問題から非常に困難になってきている。

まず，第一にあげられるのがeビジネスならではの問題であり，インターネットを用いるサイバー空間で起きる特有の問題である。これは【ネットワーク】といわれるインターネットそのものを構築するものがもつ本質的な問題点である。現状のコンピュータ･ネットワークではある程度の技術力をもつ人間であれば他人の送信した（メールなど）内容を簡単に盗聴したり，更新状況を把握したりすることは容易なことである。第二にあげられるのが法律･規制の問題である。eビジネスでは，1つの国だけでビジネスを行わず，様々な国を通じてビジネスを行うことも珍しくない。例えば日本にいながらアメリカ･韓国などのショッピングサイトを利用するのがこれにあたる。そうした場合，プライバシ保護の法律･規制はもちろんのこと，その考え方まで大きく違ってくる。

第三に個人情報を管理する企業の管理体制･能力の問題である。これは各国の法制度や規制が後手に回ったということもあり，十分な体制が整えられないままビジネスを展開することになってしまった。また，eビジネスを積極的に取り入れる企業の多くは，中小企業やベンチャー企業といった成長企業であり，社員教育や設備投資に多くのコストをかけることができない企業が多い。このため1つの企業で管理コストを賄うのは困難となり，十分な管理能力を有することができないでいる。これは第一の問題であげた【ネットワーク】の本質的な問題でも言えることであるが，管理コストをかけてセキュアなネットワークを構築することで，ある程度は盗聴などを防ぐことができる。しかしながら現状では1企業でそのコストを賄うことは非常に困難なことであると言える。しかしこれらの問題が解決したとしても個人情報の流出を完全に食い止めることは非常に困難なのが現状であるが，プライバシ保護という面においては保護することができると考えられる。またプライバシ保護の問題はこれら以外にも様々な要因があげられると思うが，大きくはこの3つであると言えるのではないだろうか。このことから，この3つの問題に重点をおいた個人情報管理の新方式を次章で論述する。

2. 個人情報管理の新方式

はじめに，従来方式と我々の提案する新方式の個人情報管理の仕組みについてショッピングサイトを例に挙げて比較していきたい。従来方式の仕組みでオンラインショッピングを利用すると，最初にサイトで購入商品を選択後，購入に必要な情報を入力する。そしてその情報を当該サイトに送信し，そこから決済情報はクレジット会社へ，配送情報は配送会社へと送信される。

この方式だと，eコマース･サーバに顧客の全ての情報が蓄えられてしまう。こうなるとeコマース･サーバが悪意あるユーザからの攻撃や，サーバ管理者の不手際があった際に個人情報がいとも簡単に流出してしまい，プライバシ保護に大きな問題が発生してしまう。そこで我々の考える方式は，はじめから

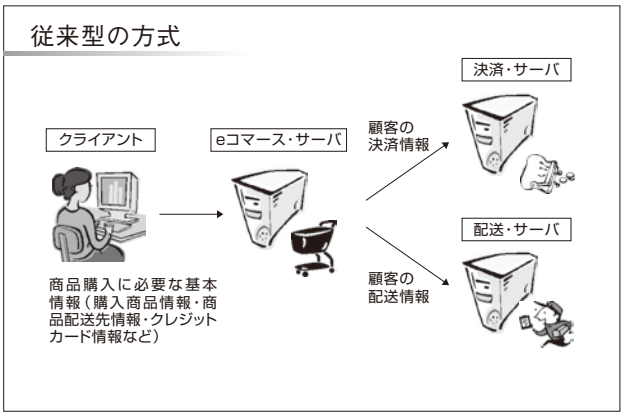
個人情報を分割し，それぞれに必要な情報以外を持たせないことにより，1つのサーバから情報が流出したと仮定しても個人を特定することは困難にする方式である。仮に一部のサーバから個人情報が流出したとしても，個人を特定するには困難な情報になる。これにより顧客のプライバシが守られる仕組みになる。

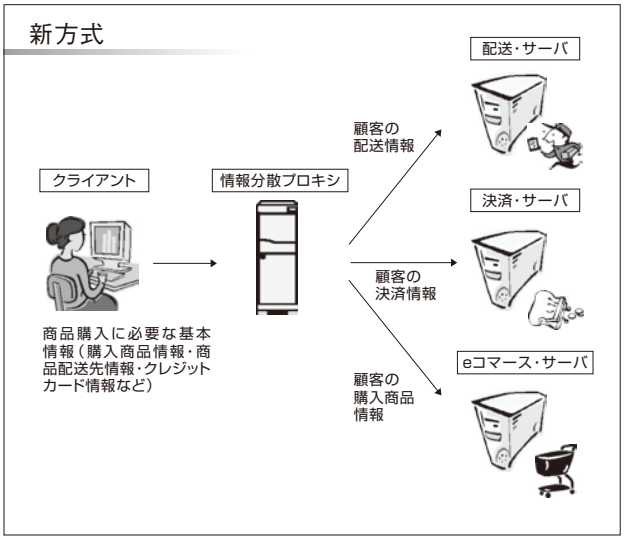
右記の図でeコマース・サーバが行っていた役割を情報分散プロキシと呼ばれるサーバにさせることで，情報を分散させ，個人情報によるユーザの識別を不可能にする。

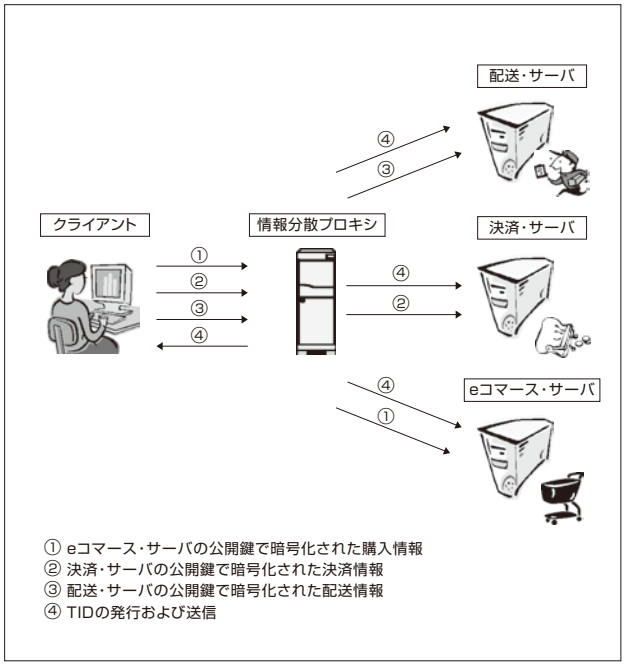
また開示される情報は，開示されるサーバの公開鍵で暗号化を行う。このため，開示されるサーバのみが情報にアクセスできる（決済情報は決済・サーバの公開鍵で暗号化される。このため配送・サーバとeコマース・サーバのもつ鍵では決済情報の暗号化を解くことができない）。また情報分散プロキシには復合化のための鍵を一切もたせないので，情報分散プロキシから情報の漏洩が起こったと仮定しても，実際の個人情報は暗号化されたままのものであるので保護される。しかしこれでは情報が別々になってしまい，どの情報と，どの情報がリンクしているのかわからなくなる問題が発生する。この問題はトランザクションID（以下TID）と呼ばれる整合性を保つための特殊なIDをそれぞれのデータに付加することで回避することができる。

またTIDは暗号化せずに送信されるが，このTIDは単体ではただの数字でしかないので漏洩したところでさほど問題ではない。また，このシステムの実装はJavaとJavaScriptを用いて開発されているのでクライアント側に一切負担をかけないシステムとなっている。

このシステムのプロセスは登録プロセス，利用プロセス，処理完了プロセスの3つのプロセスに分類される。まず登録プロセスでクライアントが購入に必要な情報を入力し，情報分散プロキシに送信する。この際，JavaScriptを用いてブラウザ上で暗号化を行う。その後，ユーザが商品購入を決定した後，入力データに不備がないことを確認し， 暗号化されたデータにTIDを付加し，情報分散プロキシに保存する。その後，利用プロセスに移行し，情報分散プロキシに保存されているTIDと各情報が各サーバに送信される。このときにデータの整合性を確保するため，各サーバに設けられた1次キャッシュ領域にデータが一時的に保存される。最後に処理完了プロセスに移行する。このプロセスではeコマース・決済・配送の3サーバからそれぞれ情報分散プロキシにTIDを送信する。そのTIDがすべて一致すれば情報分散プロキシから処理完了通知を各サーバに送信する。各サーバは処理完了の通知を受け取ったら1次キャッシュ領域に一時的に保存されていたデータを各データベースへ保存し処理を完了する。また，この一連の動作で不手際が発生した場合などのデータは，ある一定の時間が経過す







ると自動的にサーバから削除される仕組みを提供する。この新方式を採用することで，前述した問題を克服することができると我々は考えている。

まず盗聴･傍受に関しての問題であるが，これは情報そのものに価値をもたせないことで盗聴･傍受されたとしても被害を最小限にとどめることができると言える。次に法律･規制の問題であるが，上記を例にして考えると3つのデータが揃わないと個人情報として意味をなさないことがわかる。そうなれば各サーバの管理企業がすべて違う国であったとしても特に問題が生じることなく運営することができる。最後に企業の管理体制･能力の問題であるが，いままではeコマースに個人情報が集中し，管理する企業に負担が重く圧し掛かり，個人情報の漏洩がプライバシの侵害へと繋がったが，この方式であれば必要な情報以外管理する必要がない。このようにいままで単独で管理していた個人情報を複数の企業で管理し，管理する企業それぞれの情報はまったく異なるといった形態を作り上げることで，いままでの管理コスト･漏洩時の責任なども分散することができる上，仮に個人情報が漏洩した場合でもプライバシの侵害にまで繋がることが難しくなり，eビジネスを行う企業の負担を軽くすることができる。それと同時にオンラインショッピングを利用するユーザにとっても，今まで通りの手法で利用でき，「自分の個人情報が漏洩し，プライバシが侵害されるのではないか」という不安を軽減させることができると言えるのではないだろうか。これが我々の考えるプライバシ保護の新しい方式である。

3. 類似研究との比較

この章では前述した我々の方式と類似した方式を紹介する。情報処理学会が発行している『情報処理 2006 4月号 Vol.47NO.4通巻494号』「セキュリティとプライバシを両立させる匿名認証技術について」で述べられている方式がある。これは我々の方式と考え方が類似している。しかしその手段が異なる。ここで紹介されているのはグループ認証と呼ばれる方式である。これはアクセス権のある人をグループ化し，このグループに属しているかどうかでアクセスを許諾する方式である。暗号化をする際にグループで共通のパスワードや秘密鍵を配布し，それをもって秘匿するという方法であるが，この方式には大きな問題があると言える。本来グループと呼ばれるものは変動の激しいものである。そのグループに共通の鍵やパスワードを持たせても，めまぐるしく変動するグループの管理に秘密鍵やパスワードを動的に変更し続けるといったセキュリティ技術は現在は存在しない。

4. 本方式の問題点及び今後の課題

この章では我々が提案する新方式の問題点と今後の課題について述べたい。この方式はまだ研究開発段階で，すべての機能が実装されているわけではない。現状，技術面ではとくに目立った問題点は生じていないが，今後どうなるかまだ予測がつかない。しかしながら，この新方式は既存の技術を多く用いており，その活用の仕方を工夫しているため，技術面で大きな問題が発生するとは考えにくい。技術面で問題が出るとすれば，既存のeコマースサイトにこの方式を採用し，既存システムと連動する実装段階で発生すると考えられる。これはeコマースサイトが似通っているが，まったく同じものが存在せず，また実装されているプログラミング言語も違っているため，実装予想がしにくいという点から生じている問題である。しかしながら，この問題はeコマースサイトのサンプルを多く集め，十分な検証を行うことである程度解決できる問題ではある。次にあげられる課題は，既存のシステムと連動させるためのモジュール開発である。これはとくに決済システムに言えることであるが，決済会社は独自のシステムを用いている場合が多く，これらのシステムを変更せずに情報をやり取りできるインターフェースの開発が必要となってくる。これらは今後XML･XMLデータベースなどの冗長性の高い技術を用いて部分的に開発していく考えである。最後にあげられる問題は，この方式では本稿の例をあげるとショッピングサイトでは決済会社･配送会社･eコマース運営会社の3社が協力して個人情報を管理するという図式になっている。このような場合，不本意ながらもこの3社は協業体制を作らなければならなくなる。ビジネス的な観点ではこれはあまり例のないことであるので，この協業体制をいかにして作り上げることができるかが本稿の方式を成功させる問題および課題であると言える。

参考文献
[1] NPO 日本ネットワークセキュリティ協会 - 2005年度 情報セキュリティインシデントに関する調査報告書
[2] NPO 日本ネットワークセキュリティ協会 - 2003年度 情報セキュリティインシデントに関する調査報告書
[3] “情報処理 2006 4月号Vol.47NO.4通巻494号” 情報処理学会発行, 2006.4.
[4] William Stallings, 石橋 啓一郎ほか（訳）, “暗号とネットワークセキュリティ - 理論と実際” Pearson Education Japan出版, 1999
[5] Sun Microsystems, Inc. , “Webセキュリティ･プログラミング for Java テクノロジー” Sun Microsystems出版, 2002.
[6] 黒川 信弘, “セキュア社会実現へ向けての7つの提言 ー安心と信頼に支えられたIT社会実現のためにー” 日本セキュリティマネジメント学会 投稿論文, 2003.