条件付きIDを利用したネットショッピング方式

菊池幸一[†] 高見一正[†]
後藤真一郎[††] 水野修[††]

インターネット利用者のうち，ネットショッピングの利用経験のある者は89.1%と広く普及している．一方で，ショッピング会社の個人情報の流出が問題になり認識が高まりつつある．本稿では条件付きIDを応用して個人情報を暗号化することで，必要な相手以外に個人情報を知られずにネットショッピングを行う方式について提案する．

Internet Shopping System Using the Cryptographic ID Technology

Kouichi Kikuchi,[†] Kazumasa Takami,[†] Shinichiro Goto[††]
and Osamu Mizuno[††]

Internet shoppers have become widespread comprising 89.1% of all Internet users. Moreover, the leakage of personal information from shopping service providers causes a social problem, and requirements for personal information protection are increasing these days. An Internet shopping system is proposed to prevent leaking personal information such as name, home address, age, or gender using cryptographic ID technology.

1. はじめに

インターネットショッピングは，インターネット利用者全体のうち90%近く[1)]まで普及している．一方で，ユーザから見たネット上の店舗（以下，ショッピング会社と呼ぶ）等による個人情報の流出が社会問題になり，個人情報の管理の重要性に関しての認識が高まりつつある．従来のネットショッピングでは，ショッピング会社が顧客の情報を一元的に管理していることが多く，高い管理能力が求められている．しかし，実際のネットショッピングは，ショッピング会社以外に，配送会社や決済業者等，複数の事業者が関与している．そして顧客の個人情報には，商品を配送する際に必要な名前，住所等の配送会社が必要とする情報と，ショッピング会社が必要とする年齢層，性別等のマーケティング情報がある．このように，ネットショッピングに関わる企業によって，利用する個人情報が必ずしも一致しない．このため，データベース（以下，DB）による個人情報の一元管理は，原本管理等の情報の管理については優位であるが，異なる企業からのアクセス制限を施す等のコストが必要となってくる．

また，各企業が独自のDBを構築する運用も考えられる．このケースでは，ユーザ情報の更新同期等，運用に関わる問題が発生する．

さらに近年，個人情報の流出事件が多発しており，各メディアでさかんに報道されている．情報通信白書[1)]によれば，新聞5紙の個人情報流出を取り上げた記事の件数は，平成13年の118件から16年の510件と約4倍にも増大し，非常に注目されている．利用者個人についても，個人情報の問題に関心がある人の割合は97.4%を占め，個人情報に対する関心が高まっている．

このため，ネットショッピング会社には，個人情報の保護のために高いセキュリティと，管理を行う社員の知識とモラルが要求される．しかし，規則の遵守や運用方法に頼るだけではなく，技術的にも個人情報を保護できる方式を用いることが，顧客の安心と信頼を獲得するためには肝要である．

今後のネットショッピングがより重要な位置を占めるためには，個人情報の入力の煩雑性，個人情報の管理方法の2つの課題を解決することが必要である．

本稿では，このことに着目し，ネットショッピングに必要となる個人情報を利用する企業別に区切って符号化，暗号化し，条件付きIDを用いたメールアドレスとして適用する方式を提案する．これにより，ユーザは個人情報入力の煩雑性削減と必要な相手以外に個

† 創価大学工学部
Faculty of Engineering, Soka University
†† NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories, NTT Corporation

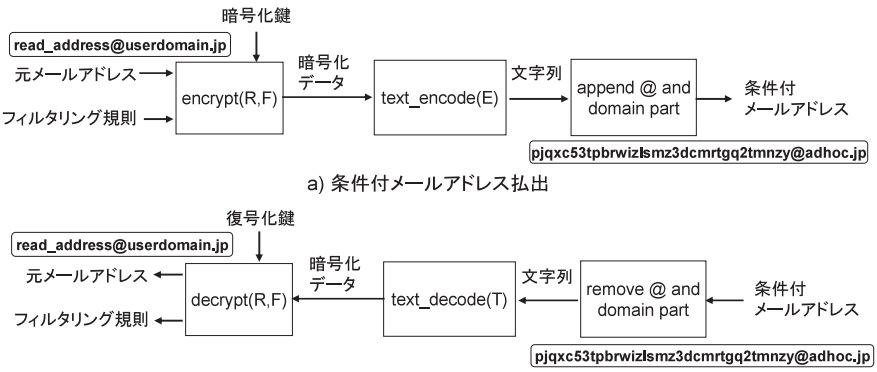

図 1 条件付き ID を利用した e-mail アドレス[2)]
Fig. 1 Cryptographic ad hoc e-mail address [2)].

人情報を知られずにネットショッピングを行うことができ，また企業での管理対象情報の簡易化が可能となる．さらに，提案方式を試作し，サービスの実装検証および情報圧縮法の影響評価を行う．まず，2 章では，条件付き ID の技術について概説し，3 章では，従来のネットショッピングの現状と問題点について示す．4 章は，条件付き ID を利用したネットショッピング方式を提案する．5 章は，サービスの実装上の課題と解決策について述べ，6 章では，サービスの実装と評価を示し，7 章で本稿をまとめる．

2. 条件付き ID 技術

条件付き ID は，複数の情報を埋め込んで暗号化し，ASCII 文字列化したものおよびその文字列を生成する技術である．条件付きメールアドレス[2),3)] を例に，条件付き ID の払い出しと検証方法を**図 1** に示す．元のメールアドレスとフィルタリング規則とが与えられると，最初にアドレス発行機能はこれらの情報を暗号化する．暗号化データは BASE32 符号化規則[4)] により ASCII 文字列に変換され（図 1 の a)），ドメインが付加される．このときのドメインは，転送時にアドレスセンタを経由するためのものである．このメールアドレスでメール送信すると，メール送信機能はそのアドレスから元のメールアドレスとフィルタリング規則を抽出し（図 1 の b)），メールを元アドレスへと転送する．条件付き ID の利点は，複数の個人情報を埋め込むことによりそれ自身を個人情報のデータレコードと見なすことができるので，DB が不要になるということである．DBMS（Database Management System）との性能比較を行った結果，条件付き ID に対するシステムの処理は高速かつ低負荷で実施されることが別途報告されている[5),6)]．したがって，この技術を用いることでサービス提供者はユーザの個人情報の管理負担を低減させることができるほか，DB への多重アクセスに起因するシステムの負荷を低減させることが可能となる．

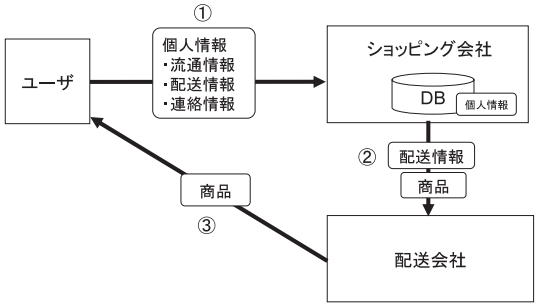

図 2 従来のネットショッピング方式
Fig. 2 A traditional internet shopping system.

3. 従来のネットショッピング方式

従来のネットショッピング方式の概要を**図 2** に示す．従来方式では，① ユーザが商品購入時にショッピング会社に個人情報を通知すると，② ショッピング会社は配送会社にユーザの住所，名前を知らせ，商品を渡して配送依頼する．そして ③ 配送会社は商品をユーザに届ける，というのが一連の処理の流れである．また，② のフェーズにおいて，ショッピング会社が配送会社から商品購入ごとにユーザの住所に相当する識別符号[7)] を取得する方式も提案されている[8)]．ユーザが商品購入時に登録する個人情報について，各ショッピング会社によっては DB 等による管理を行うところと，行わないところがある．

後者は，ショッピング会社のコストは軽減できるが，ショッピングのたびに毎回入力を求められるため，ユーザにとっては非常に手間がかかる．それに対して，前

者は，DB による個人情報の管理をショッピング会社が行っているため次回の利用の際に個人情報の入力を求められることはない．しかし，たとえば配送を別の会社が行う場合，その個人情報のうち配送時に必要な情報（住所等）は，ショッピング会社には直接必要なく，配送会社のみが知っていればよい．ショッピング会社がショッピングに必要なすべての個人情報を管理することになり，それが流出した際の危険性が非常に高くなる．また，識別符号を用いる方式は差出人と受取人の個人情報を直接相互に開示する不安感を排除することはできるが，ショッピング会社および配送会社は住所等の個人情報を DB で管理しており上記の問題の解決には至っていない．

4. 条件付き ID を利用したネットショッピング方式

本稿では，個人情報を以下のようにとらえる．なお，支払情報（たとえばクレジットカードの情報）については，購入する商品に応じて支払手段が選択できるように，条件付き ID として暗号化する個人情報からは除外した．したがって，支払情報は，従来と同様にそれぞれの決済会社が管理・保持することを想定している．

1）配送情報：配送会社が配送業務を行うために必要な情報．名前，住所等がある．
2）流通情報：ショッピング会社がマーケティングを行うために必要な情報．年齢，性別等がある．
3）連絡情報：ショッピング会社・配送会社がユーザと連絡をとるために必要な情報．メールアドレス等．

配送会社以外には，住所や名前等の情報は必要なく，ショッピング会社以外には，購入年齢層，性別等の情報は必要ない．つまり，1 つの情報源から相手の立場によって取り出せる情報が異なるような仕組みをつくれば，ショッピング会社の DB で顧客の住所等の必要ない情報が流出する被害が大幅に減ることが予想される．

そこで本稿では，条件付き ID を利用して配送・流通情報を暗号化し，情報が必要な相手にのみ復号化されて情報を受け取らせることができる情報源とする方法を提案する．この条件付き ID をユーザが次回の購入時にショッピング会社に提示することにより，再度個人情報を入力する必要がないため，煩雑性も解決される．また，本稿では，配送・流通情報のすべてを条件付き ID に梱包することにより，ショッピング会社が DB を管理する必要をなくすこととする．もちろん，発行サーバにおいても配送・流通情報のすべてを条件付き ID として梱包しているので，DB としてこれらの情報を管理する必要もない．さらに，条件付き ID

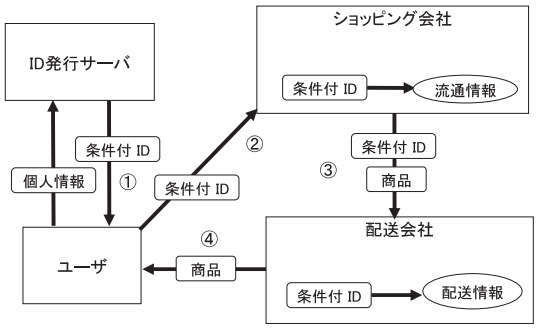

図 3 条件付き ID を利用したネットショッピング方式
Fig. 3 Internet shopping system using Cryptographic ID.

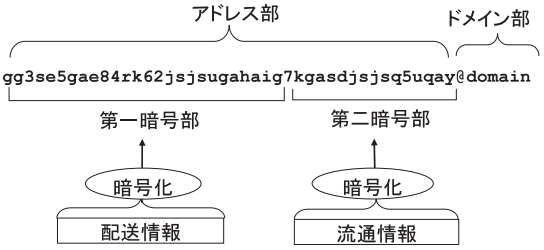

図 4 複数の条件付き ID を連結したメールアドレス
Fig. 4 Mail address of two concatenated cryptograms.

をメールアドレスとすることにより，そのままショッピング会社や配送会社がユーザとの連絡に使用することができるため，本方式ではこの払い出しするメールアドレスそのものを連絡情報として用いる．本方式の概要を**図 3** に示す．

① ユーザが発行サーバに配送情報，流通情報をつけて発行依頼を行うと条件付き ID をメールアドレスの先頭から@までの文字列（以降，アドレス部）に付加したメールアドレスが発行される（**図 4**）．なお，発行サーバには配送情報，流通情報は管理せず，条件付き ID 発行のための暗号化のみを行う．
② このメールアドレスを購入時にショッピング会社へ通知するとショッピング会社があらかじめ所持している復号化システムを使ってメールアドレス中の条件付き ID を復号化し，流通情報を読み出す．
③ ショッピング会社が ② で受け取ったメールアドレス（条件付き ID）を配送会社に通知し，商品を受け渡し，配送依頼を行う．配送会社も復号化システムを使い，ショッピング会社が受け取った情報とは異なる配送情報を読み出す．
④ 配送会社は配送情報からユーザに商品を配送する．

本提案方式では，情報を必要とする相手（ショッピング会社，配送会社）によってメールアドレスの一部

分だけが暗号化・解読できる機能を持たせ，必要な情報だけが相手に伝わるような機能が必要である．

そのため，本方式では図 4 に示すように，2 つの異なった条件付き ID を連結したメールアドレスの払い出しを行う．

しかし，メールアドレスのアドレス部には最大長 64 バイトという制限がある[9]．そこで次章では，本方式を実装するにあたり，アドレス部に格納する個人情報の種別の選択とその圧縮する方法について述べる．

5. 個人情報の圧縮方法

5.1 許容情報量の算定

アドレス部における配送情報のバイト長を α，流通情報のバイト長を β とすると，アドレス部のバイト長 γ は条件 (1) に示す関係が成り立つ．

$$\gamma = \alpha + \beta \leqq 64 \qquad \text{条件 (1)}$$

暗号化データを文字列化するのに BASE32 符号化方式[4] を用いたので，$\gamma = 64$ のとき暗号化データ Γ のバイト長は

$$\Gamma = 64 \times 5/8 = 40$$

となる．また，部分暗号化機能を実装するために各条件付き ID に 6 バイトのヘッダ情報が必要となる．したがって，配送情報・流通情報の暗号化データのバイト長をそれぞれ A，B とすると

$$A + B \leqq 40 - 6 \times 2 = 28 \qquad \text{条件 (2)}$$

となり，A，B 合わせて 28 バイト以内におさめなければならない．

5.2 ネットショッピングでの登録情報分析

ショッピング会社での，商品購入時の代表的な注文フォーム例を**図 5** に示す．このような注文フォームを対象に，大手ポータルサイトや，インターネットを利用したショッピング会社 10 社を参考に入力を求められる情報の頻度を調査した．生年月日と年齢等，近い意味を持ったものは 1 回としてカウントし，ショップごとの細かなアンケート（主に医療，健康関係）等は，結果に影響しないためカウントしないものとした．調査結果を**表 1** に示す．表 1 より，郵便番号，住所，名前，電話番号，生年月日，メールアドレスが 10 件中 10 件とすべてのショッピング会社で必要であり，性別，職業もほとんどの場合に必要になることが分かった．したがって，「郵便番号，住所，名前，電話番号（固定，携帯），生年月日（年齢），性別，職業（職種）」の 7 種類をネットショッピングに必要な個人情報として条件付き ID 化すればいいことが分かった．このうち配送に必要なのは (a)「郵便番号，住所，名前，電話番号」，マーケティングに必要なのは (b)「生年月日，性別，職業」である．本稿では (a) を配送情報，(b) を流通情報とする．このうち次節では，最もバイト長を有すると考えられる氏名と住所の圧縮方法について詳細に述べる．

図 5 注文フォーム例
Fig. 5 An example of order entry form.

表 1 ショッピング会社がユーザに入力させる個人情報の件数
Table 1 Personal information to be entered by a user.

項目名	件数
郵便番号	10
住所（丁目、番地、ビル名）	10
名前（姓、名）	10
電話番号（固定、携帯、FAX）	10
生年月日（年齢）	10
メールアドレス（PC、携帯）	10
性別	9

項目名	件数
職業（業種、会社名、役職）	8
定期的なメールの購読	4
意見・質問	2
血液型	2
タイムゾーン	1
既婚・未婚	1
出身地	1

5.3 氏名の圧縮方法

氏名の情報フィールドの長さを考える際，その文字数，文字の種類のばらつきが著しいことから，少ない情報量ですべての氏名を表現することは困難である．存在する氏名の最大長に対応しない限り，限られた情報量で名前を表現するとき，ある程度はサービスに適応できない名前が出てくることが考えられる．日本人の名前の文字数の傾向として，姓が 1〜3 文字，名が 1〜3 文字の範囲に収まっている人が圧倒的に多く，姓・名双方ともがこれよりも長い（= 氏名が 7 文字を超える）人は，ごくまれにしかいない．そこで，学生約 19,200 人を標本に氏名の文字数の調査を行った．その結果を**表 2** に示す．平均 4.0474 文字，標準偏差 0.5473 文字，6 文字以内の氏名は全体の 99.84%を占めることが分かった．6 文字以上の氏名はわずか 0.16%であるが存在しており，その内容を分析すると，以下の 3 つのケースであった．

(a) 名前がアルファベットで登録されている場合
(b) 第一，第二水準漢字にあてはまらない漢字を含む場合
(c) 7 文字以上の文字で表現される場合

文字数オーバする名前は，外国，日系人のカタカナで表現される名前がほとんどであり，漢字のみで表現されているにもかかわらず 6 文字を超える名前は

表 2 全学生の氏名の文字数
Table 2 Number of character of 19,200 students' name.

文字数	構成比
2文字	0.28%
3文字	11.12%
4文字	72.96%
5文字	15.18%
6文字	0.31%
7文字	0.04%
8文字	0.07%
9文字	0.03%
10文字	0.02%
合計	100.00%

表 3 EUC コードの変換の例
Table 3 Conversion of EUC code.

JIS コード		文字	変換前		変換後
16	1	亜	B0A1	→	1410
16	2	唖	B0A2	→	1411
16	3	娃	B0A3	→	1412
16	4	阿	B0A4	→	1413
16	5	哀	B0A5	→	1414
16	6	愛	B0A6	→	1415

0.005%だけであった．氏名の 6 文字制限は，カタカナやアルファベット表現等，漢字以外の文字を含む名前に対して非常に弱いが，ほとんどの日本人の氏名に対応できるため，本稿では氏名の最大 6 文字（12 バイト）の制限を設定する．

日本語 EUC コードでは記号，ひらがな，カタカナ，第一水準漢字，第二水準漢字を 7,808 パターンで表現している．そこで，氏名にはひらがな・カタカナ・第一，二水準漢字のみを用いることとし，利用しない文字コードを切り捨て，1 文字あたり 2 バイト（65,536 種）表現を**表 3** に示すように変換を行うことで，13 ビット（8,192 種）で表現できる．さらに 256 進数（1 バイト）で基数変換を行う．これにより氏名が 10 バイトで表現できる．

5.4 住所の圧縮方法

現在，郵便局では住所をバーコード[10] として印字し，仕分けの効率を上げるサービスを行っている．その概要は郵便番号と住所から数字（13 桁で構成される住所表示番号，13 桁に満たない場合はパディングされる）を抜き出したものをつなげ，コード化したものである．実際の変換方法を**図 6** に示す．

つまり，住所すべてを格納する必要はなく，(a)「郵便番号」と (b)「丁目，番地，部屋番号等」があれば

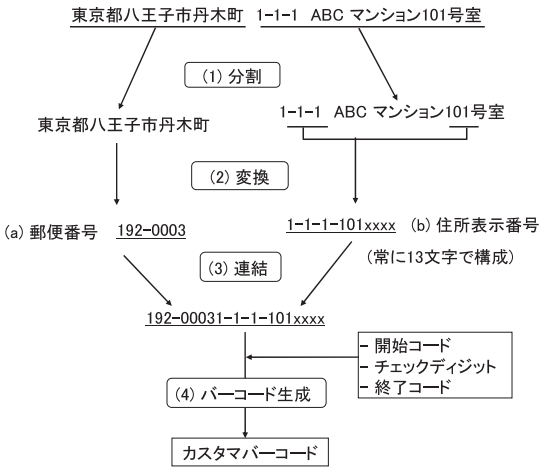

図 6 住所のカスタマーバーコード化の手順[10].
Fig. 6 Procedure of formation of user bar code of home address [10].

表 4 圧縮結果
Table 4 Result of compression.

項目	変換前		変換後
郵便番号	8バイト	→	3バイト
住所	約500バイト	→	6バイト
名前	12バイト	→	10バイト
電話番号	13バイト	→	5バイト
誕生日	10バイト	→	2バイト
性別	2バイト	→	1ビット
職業	約20バイト	→	7ビット
合計	約600バイト	→	27バイト

注：住所の圧縮後の情報量は住所表示番号のみの値

配送物が届くことになる．(b) は住所表示番号と呼ぶ．これを参考に住所を数字と区切りを示すハイフンのみで郵便番号を除いた住所を表現することができる．住所表示番号は，0〜9 の数字とハイフンで表現されるため 11 進数 13 桁として扱うことが可能である．これを名前と同様に 256 進数（1 バイト）で基数変換を行う．これにより住所が 6 バイトで表現できる．

このほか，郵便番号・電話番号・生年月日は，整数のみを取り出した 10 進数を 256 進数（1 バイト）に基数変換して表現し，それぞれ 3 バイト，5 バイト，2 バイトに圧縮する．

性別は男・女の 1 ビット，職業は必要な選択肢をコード化して 7 ビットで表現する．以上の結果を**表 4** にまとめる．以上の圧縮方法により圧縮前は最大 600 バイト程度の情報量を圧縮後には 27 バイトまで減らすことができ，条件 (2) を満足する．また，以上より

$$A = 3 + 6 + 10 + 5 = 24$$

$\therefore \quad \alpha = \mathrm{ceil}((24+6)/5) \times 8 = 48$

$B = 2 + 1 = 3$

$\therefore \quad \beta = \mathrm{ceil}((3+6)/5) \times 8 = 16$

となる．$\mathrm{ceil}(x)$ は x を切り上げる関数である．

6. 評　　価

6.1 実験システム

条件付き ID を利用したネットショッピング方式は，

① ユーザは，ブラウザ等を利用してサーバからメールアドレス（条件付き ID）を受け取る，

② ユーザは，受け取ったメールアドレスをショッピング会社の注文フォーム上で入力する，

③ ショッピング会社は，検証プログラムを使ってメールアドレスから流通情報を手に入れる，

④ ショッピング会社は，注文された商品とメールアドレスを配送会社に渡す，

⑤ 配送会社は，検証プログラムを使ってメールアドレスから配送に必要な情報を手に入れる，

⑥ 配送会社は，商品をユーザに配送する，

の 6 つの手順で行われる．

このうち，①，②，③，⑤ の 4 つを実装し，実現可能性および評価実験を**図 7** に示すような環境で行った．

6.2 個人情報の情報量の比較

本方式では個人情報を 27 バイトに圧縮することができる．実際にゼミ生 10 人分の個人情報を入力し，圧縮前の情報量と圧縮後の情報量の比較を行った結果，10 件分の個人情報の情報量の総和は 1,269 バイトであった．

この 10 件を条件付き ID に付与して本方式のメールアドレス払い出しを行うと，1 人あたり 64 バイト × 10 人 = 640 バイトとなるので，圧縮前よりも情報量が減少していることが分かる．

6.3 圧縮・解凍処理による処理速度への影響

これらの圧縮・解凍処理を行うことで払い出し・検証の処理にどの程度影響を与えるのか調べる必要がある．そこで，1,000 件の情報を処理する際の処理時間計測した．

この処理時間の測定には，1 つの個人情報を圧縮のみ行うプログラム，圧縮後暗号化するプログラム，また，これらで作成した圧縮・暗号化した情報を引数として，解凍（配送情報と流通情報の 2 種類）のみ行うプログラム，解凍後復号化するプログラムを実行する．これらを内部処理で，1,000 件の処理を 20 回行わせて処理にかかった時間を毎回測定し，その平均値をとった．実行したマシンのスペックは CPU 2.4 [GHz]，メモリ 256 [MB]，OS は Windows XP で，実行時には負荷はかけていない．

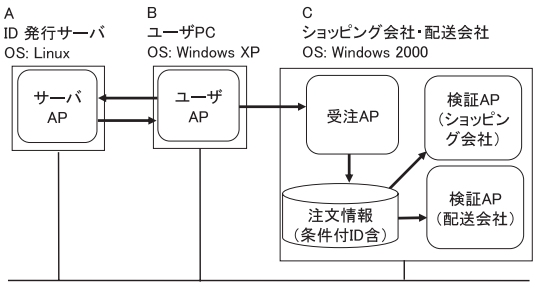

図 7 サービスの実行環境
Fig. 7 Experiment of system.

表 5 圧縮・解凍処理の 1,000 件あたりの処理時間
Table 5 Processing time on compression and extraction of personal information.

（単位：[ms]）

圧縮		解凍（配送情報）		解凍（流通情報）	
圧縮のみ	＋暗号化	解凍のみ	＋復号化	解凍のみ	＋復号化
744	13,020	794	3,117	2.82	1,738

実験の結果を**表 5** に示す．圧縮は約 0.74 [ms/件]（圧縮 + 暗号化の処理時間に対して 5.7%），配送情報の解凍は約 0.79 [ms/件]（復号化 + 解凍の処理時間に対して 25.5%），流通情報の解凍は約 2.9 [ns/件]（同 0.17%）で処理することができた．6.1 節で示したサービスの流れの中で ②，④，⑥ はユーザ，ショッピング会社，配送会社の入力および業務遂行速度に依存するので，①，③，⑤ をサービス全体の処理時間として想定できる．① の圧縮 + 暗号化処理時間は 13 ms/件，③ の流通情報の復号化 + 解凍処理時間は 1.7 μs/件，⑤ の配送情報の復号化 + 解凍処理時間は 3.1 ms/件．なお，配送情報については最終的にラベルを印刷すると想定すると，印刷にかかる時間は，最新のラベル印刷機[11),12)] で 100〜150 mm/秒である．100 mm がラベルの大きさと考えると，1 枚の印刷時間は約 670〜1,000 ms，であり，全体としては 673.1〜1,003.1 ms/件と想定される．したがって，①+③+⑤ の時間は 686.1〜1,016.1 ms/件となり，想定サービス時間の支配要因はラベルの印刷時間であり，提案方式の処理はこの中の 1.6〜2.3%である．このことから圧縮・解凍の処理時間は，サービス全体の処理時間に対して影響はそれほどないことが分かる．

以上から，本方式の有効性を確認することができた．

7. おわりに

7.1 本提案方式の実現可能性について

近年大幅に増加したネットショッピングの利用者

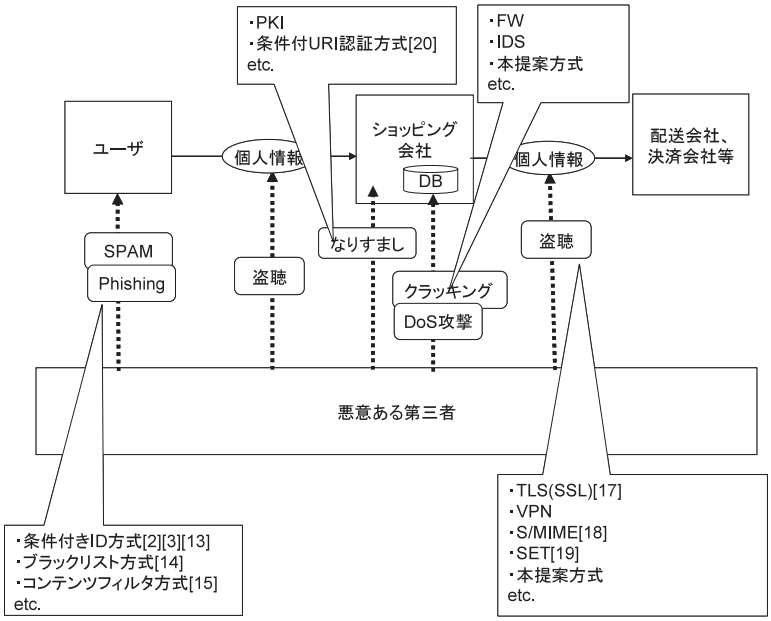

図 8 電子商取引における脅威とその対策
Fig. 8 Threats and their solutions in electronic commerce.

と，一般ユーザの個人情報に対する意識の高まりから，ショッピング会社での注文情報入力の煩雑性を回避するための個人情報を管理が重要な課題となっている．本稿では，個人情報の流出の危険性を低下させ，ユーザの注文情報入力の煩雑性を改善するために，ショッピング会社・配送会社に個人情報を暗号化した ID を渡し，業者ごとに必要な個人情報のみを取り出せる条件付き ID を利用したネットショッピング方式を提案した．

また，ネットショッピングに必要な個人情報を調査し，郵便番号，住所，名前，電話番号が配送会社には必要であり，生年月日，性別，職業等についてほとんどのショッピング会社が入力を求めてきていること示した．これにより，これらの情報を配送情報と流通情報とし，別々に暗号化した後，1 つの ID として連結することによってそれぞれの業者が必要な情報だけを復号化して個人情報が得られる方式を提案した．また，各業者との連絡方法として条件付き ID をメールアドレスとして利用できるように，64 文字に制限されているアドレス部に制限内で設定できる情報圧縮法を提案した．そしてサービスの実装を行った結果，圧縮・解凍処理は，サービス全体の処理速度の低下にあまり影響を与えないことを確認した．

また，提案システムの拡張として，流通情報に地域（住所）も加えたい場合には，ショッピング会社の復号システムに配送情報も解凍できる機能を具備すれば実現でき，情報選択の柔軟性への対応も可能である．ただし，表 1 で条件付き ID 化から除外した 6 項目については，ショッピング会社ごとで独自性が強い流通情報であり，また個人情報としての保護が必要な項目は少ない．したがって，従来どおりユーザによる入力が必要であるが，必須情報ではないため，入力の煩雑性改善への影響は少ない．

7.2 本提案方式がカバーするセキュリティ上の脅威について

電子商取引における脅威は**図 8** に示すように 3 種類の脅威があるととらえられ，それぞれにおける様々な対策が提案されている．

1) ユーザへの脅威：SPAM メール，フィッシング等．解決策として条件付きメールアドレス方式[2),3),13)]，ブラックリスト方式[14)]，コンテンツフィルタ方式[15)]，3way 発信者認証方式[16)] 等が提案されている．
2) ユーザ–ショッピング会社間，ショッピング会社–別会社（配送会社等）の情報流通の間における脅威：盗聴．
   解決策として TLS（Transport Layer Security）[17)]，VPN（Virtual Private Network）等，通信路を暗号化する方式，S/MIME [18)]，SET [19)] 等，送信する情報を暗号化する方式がある．
3) ショッピング会社への脅威：クラッキングによる管理情報の盗み見，DoS（Denial of Service）に

よるシステム攻撃，盗聴して取得したユーザ情報を元にユーザになりすます，等がある．

解決策としては，ファイヤウォールや侵入検知システム等による監視を行う方法と，PKI（Public Key Infrastructure）による第三者機関信用を獲得する方式，条件付き URI[20] 等がある．

このうち本提案方式がカバーしているのは 2) および 3) のクラッキング・DoS 攻撃からのセキュリティ対策であるということができる．すなわち，2) については S/MIME，SET と同じく情報を暗号化する方式であるが，S/MIME，SET に対応するシステムをユーザとショッピング会社双方に導入しなければならないのに対し，本提案方式はユーザにとっては通常のメールアドレスと同様に扱えるので利便性が高い．また，3) のクラッキング・DoS 攻撃については，本提案方式を用いることによりショッピング会社は DB を持つ必要がなくなるため，情報漏洩の危険性がなくなるだけでなく，DoS のような多重アクセス攻撃により発生する DBMS 起因のシステム負荷が低減されるため，攻撃そのものの意味が消失するという利点がある．また，1) の脅威については，以下のようにとらえられる．SPAM メールについては，悪意ある第三者が自動生成したメールアドレス宛にメール送信した際に偶然実在するユーザのアドレスに合致してしまうケースと，何らかの手段で取得したユーザのメールアドレス宛にメール送信するケースの 2 通りが考えられる．前者のケースについては，本稿提案のメールアドレスは十分に長く，かつ第三者が辞書等を用いて類推することができない形式であるため，運用上防御可能である．また，後者のケースについては，本稿提案の条件付きメールアドレス a が第三者に漏洩しないようにすることが重要である．メールアドレスが第三者に漏洩する危険のある局面としては下記の 2 つが考えられる．

- ユーザからショッピング会社へ商品の注文を行う際に a を入力．
- 連絡のためショッピング会社，もしくは配送会社から a 宛にメールを送信する．

このうち前者は 2) の脅威への対策によりカバーされる．後者については，たとえばショッピング会社，配送会社からユーザへ送信することだけを許可する別の条件付きメールアドレス b（参考文献 2)，3) 等）を事前に払い出し，連絡の際には b を用いることにより，a が第三者に漏洩することを防ぐことが可能である．

またフィッシングについては，業者等になりすましてユーザの個人情報を引き出すことが目的である．本稿提案の方式では，個人情報が暗号化され，特定の業者（ショッピング会社，配送会社）しか復号化できない．したがって前記目的が達成されずフィッシングの意味を消失させることが可能である．

7.3 今後の課題について

残された課題について述べる．前節で触れたフィッシングについては，悪意ある第三者が条件付きメールアドレスを発行するサーバになりすまして，個人情報を不正入手する場合も考えられる．したがって，PKI 等により正規の発行サーバであることを証明する仕組みが必須となる．

一方，悪意ある第三者が不正に入手した条件付きメールアドレスを用いてユーザになりすまし，不正に商品購入を行う場合も考えられる．この場合，本人が確かに購入処理を行ったことを証明する手法を組み込む必要がある．たとえば許可されたユーザのみに見せる購入画面を条件付き URI[20] に入れ，それを別途メールアドレス宛に送信して認証する方式が考えられる．

また，本提案方式では必要な個人情報はすべて 1 つのメールアドレスに梱包しているため，本方式を個人情報の分散管理方式ととらえることができる．したがって管理責任がショッピング会社からユーザ個人に帰着することになり，ユーザの管理負担が発生するという問題がある．しかし，最近のトレンドとして，ユーザが自分のプロファイルを自分で管理し，必要なときのみに相手に提示するという方法[21] が注目されており，ユーザ自身が自分の個人情報を管理し，安全に利用できる環境が整いつつある．さらに，暗号化されているとはいえ個人の情報が 1 つに集約されているため，個人情報の安全性が暗号化方式の強度に依存しているという問題点もあり，強力な暗号化方式を選択してセキュリティを確保する必要がある．今後，管理形態や最適な暗号化方式について検討していく．

参 考 文 献

1) 総務省：平成 17 年度版情報通信白書 (2005).
2) Abe, T., Miyake, J., Kawashima M. and Takahashi, K.: Spam Filtering with Cryptographic Ad hoc E-mail Addresses, *The 2004 International Symposium on Applications and the Internet* (*SAINT 2004*), IEEE Computer Society and the Information Processing Society of Japan (2004).
3) Kawashima, M., Abe, T., Minamoto S. and Nakagawa, T.: Cryptographic Alias E-mail Addresses for Privacy Enforcement in Business Outsourcing, *ACM CCS2005 Workshop on Digital Identity Management* (*DIM 2005*), ACM Special Interest Group on Security, Audit and Control (2005).

4) Josefsson, S. (Ed.): The Base16, Base32, and Base64 Data Encodings, RFC3548, IETF (July 2003).
5) 後藤真一郎，岡本光浩，水野　修：条件付き ID を利用したサービス利用権判定方式の評価，電子情報通信学会第 1 回次世代ネットワークソフトウェア研究会—次世代ネットワークソフトウェアの技術の展望 (2005).
6) 平田直之，平井泰樹，仲光由次，後藤真一郎，石井啓之：条件付き ID とデータベースを組み合わせたサービスの利用権判定方式に関する一考察，電子情報通信学会 2006 年総合大会 B-7-179 (2006).
7) 日本郵政公社：あて名変換サービスの開始について，2006 年 7 月 6 日報道発表資料 (2006). http://www.post.japanpost.jp/whats_new/2006/topics/atena_henkan.html
8) 楽天株式会社：楽天オークションが業界初の匿名で利用可能なエスクローサービスを開発，2006 年 7 月 6 日ニュースリース (2006). http://www.rakuten.co.jp/info/release/2006/0706.html
9) Klensin, J. (Ed.): Simple Mail Transfer Protocol, RFC2821, IETF (Apr. 2001).
10) 日本郵政公社：郵便番号制マニュアル. http://www.post.japanpost.jp/zipcode/zipmanual/index.html
11) Canon LX760RF. http://cweb.canon.jp/cardprinter/colorlabel-printer/lx760/index.html
12) Epson TM-L90（業務用小型プリンタ）. http://www.epson.jp/products/tm/tml90p/index.htm
13) Spamex. http://www.spamex.com/
14) ORDB.org. http://ordb.org/
15) Yerazunis, W.S.: The Spam-Filtering Accuracy Plateau at 99.9% Accuracy and How to Get Past It, *MIT Spam Conference* (2004). http://crm114.sourceforge.net/Plateau_Paper.html
16) Mailblocks. http://about.mailblocks.com/
17) Dierks, T. and Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1, RFC4346, IETF (Apr. 2006).
18) Ramsdell, B. (Ed.): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, RFC3851, IETF (July 2004).
19) SET Secure Electronic Transaction^{TM}, Version 1.0 (May 31, 1997).
20) 佐久間美能留，白神彰則，安部　剛，高橋克巳：条件付 URI を利用したユーザ認証方式の提案，電子情報通信学会 2004 年ソサイエティ大会 B-7-56 (2004).
21) Microsoft's Vision for an Identity Metasystem. http://www.identityblog.com/stories/2005/07/05/IdentityMetasystem.htm

(平成 18 年 5 月 29 日受付)
(平成 18 年 11 月 2 日採録)

菊池　幸一

2006 年創価大学工学部情報システム学科卒業．インターネットショッピング方式とメールシステムの研究に従事．現在はコムシス株式会社に勤務．電子情報通信学会会員．

高見　一正（正会員）

1977 年静岡大学工学部電気工学科卒業．1979 年同大学大学院修士課程修了．同年日本電信電話公社（現，NTT）入社．以来，電話・パケット網間接続，マルチメディアパケット交換方式，ATM 呼制御方式の研究開発，1991 年より 3 年間 ATR 通信システム研究所にて通信サービス仕様記述法の研究，1994 年より NTT ネットワークサービスシステム研究所で高度 IN の研究開発，2001 年より，次世代 IP 網サービスの研究開発に従事．2004 年 4 月より創価大学工学部情報システム工学科教授．工学博士．電子情報通信学会，IEEE（シニア）各会員．

後藤真一郎（正会員）

1989 年早稲田大学理工学部機械工学科卒業．1991 年同大学大学院理工学研究科修士課程修了．同年日本電信電話（株）入社．以来，ソフトウェア開発効率化技術，マルチメディアサービスオペレーションシステム，IP ネットワーク課金システム，セキュリティサービス技術，パーソナルサービス技術の研究開発に従事．

水野　　修（正会員）

1983 年東京工業大学工学部電気・電子工学科卒業．1985 年同大学大学院総合理工学研究科修士課程修了．同年日本電信電話（株）入社．以来，通信サービス開発支援技術，高度インテリジェントネットワークシステム，IP サービスシステム，セキュリティサービス技術の研究開発に従事．現在 NTT 情報流通プラットフォーム研究所・主幹研究員．電子情報通信学会，IEEE 各会員．