6H-1

葉書コールバックによる認証の零細企業への応用

宮原　隆行†
上武大学ビジネス情報学部†

１．はじめに

インターネットを利用した商取引の形態は，通信販売のインターネット版から，サービスの提供へと広がった．それに伴い，従来では問題にならなかった事柄が，問題になるケースも起きている．

インターネットを利用して，物質から構成される商品を販売する商取引では，商品代と送料を顧客が入金したことを確認し，顧客が指定した住所に商品を確実に送るだけで取引が成立した．例え，顧客が住所を偽ったとしても，商品が届きさえすれば，問題は起きなかった．

しかし，インターネットを利用してコミュニケーションを行うといった情報だけを扱うサービスでは，利用者の住所氏名という情報は，必ずしも必要にならない．そのため，住所氏名の情報を伝えることなく，匿名でサービスを利用することが可能であり，利用者間でトラブルが発生し，提訴を行おうと思っても，相手が誰であるか判らないという問題が起きている．本稿では，住所氏名を特定できる葉書と，インターネットにおけるコミュニケーション手段の一つである電子メールの，二つの異なるメディアを用いることにより，サービス利用者を特定する手法を提案する。

２．情報発信者を特定する際の問題点

サービス提供者が判る情報は，情報を送信したコンピュータのグローバルＩＰアドレスだけである．過去のインターネットの世界では，グローバルＩＰアドレスは，各機関の各コンピュータに静的に割り当てられていた．そのため，情報の送信元のグローバルＩＰアドレスが判明すれば，どの機関の，どのコンピュータから送信された情報なのかは容易に突き止められた．しかし，今日では，家庭のコンピュータをインターネットに参加させるために，インターネット・サービス・プロバイダ（以下，ＩＳＰ）を利用するのが一般的である．ＩＳＰは，グローバルＩＰアドレスを節約するために，家庭のコンピュータとグローバルＩＰアドレスを１：１に割り当てず，要求があった時のみ，動的に，家庭のコンピュータと空いているグローバルＩＰアドレスを結び付けている．そのために，同じ家庭でも，割り当てられるグローバルＩＰアドレスは，接続毎に異なる．このことによって，情報を受信した側は，情報の発信元のグローバルＩＰアドレスを確認することが可能であっても，どの家庭のコンピュータから情報が発信されたのかは識別が不可能であった．

しかし，グローバルＩＰアドレスを割り当てるのは，ＩＳＰであるので，ＩＳＰが，いつ，どの家庭のコンピュータに，どのグローバルＩＰアドレスを割り当てたのかというログを残せば，情報の発信元は，特定可能になる．このログの開示を義務付けた法律が，特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律，いわゆる，プロバイダ責任法である．

しかし，ＨＴＴＰを扱うＷｅｂの世界においては，匿名で情報を中継する匿名プロクシというサービスが存在するという問題が残っている．匿名プロクシは，ＨＴＴＰで送信された情報を中継する機能を持つ．そのため，Ｗｅｂサーバのログには，情報の発信元ＩＰアドレスとして，発信者のＩＰアドレスではなく，匿名プロクシのＩＰアドレスが記録されてしまう（図１）．匿名プロクシは，世界中に存在するために，中継を行った情報の発信元ＩＰアドレスの開示を求めるのは不可能である．

匿名プロクシによる問題を防ぐために，Ｗｅｂサーバに情報が送られる度に，発信元ＩＰアドレスに対して情報送信を試みて，情報が送信できてしまう時には，匿名プロクシ経由の送信と判断し，アクセスを拒否する方法が存在する．しかし，この方法では，匿名プロクシ経由の存

A letter call back for very small office
† Takayuki Miyahara,
Faculty of Business Information Sciences, Jobu University

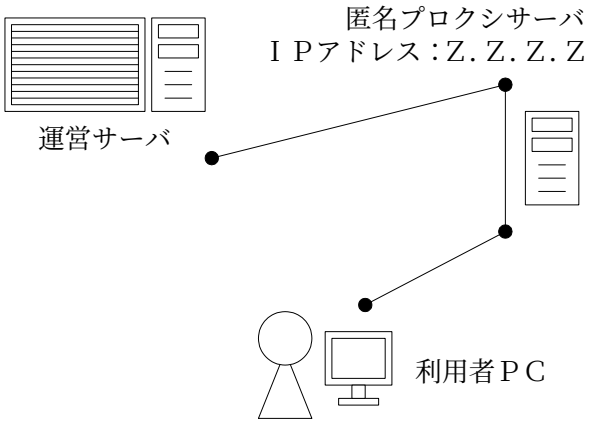

図１　匿名プロクシサーバ経由の接続

在を調べるために，無駄なトラフィックを発生させてしまう．一般にＷｅｂを利用したサービスにおいて，発信元ＩＰアドレスを，サービス利用者と結び付けることは不可能である．

プロバイダ責任法は，ＩＳＰだけではなく，情報を扱うＷｅｂ上の管理者にも関わる法律である．

そこで，Ｗｅｂを利用して情報を扱うサービスを行うにあたっては，ＩＰアドレス以外の情報を用いて認証を行い，情報発信者を特定しておくことが望ましい．なお，プロバイダ責任法で明示的に定められている発信者情報は次の通りである．

1. 発信者の氏名
2. 発信者の住所
3. 発信者の電子メールアドレス
4. ＩＰアドレス
5. 時刻

上記１と上記２が特定できれば，提訴を行うことが可能になるため，最低限必要な情報は，上記１と上記２の情報である．認証には，電子的な鍵を用いることとすると，第三者に鍵が盗まれないように鍵を送付することも課題となる．

まず，考えられるものが上記３の電子メールを使用した鍵の配布である．電子メールに含まれた鍵を読むことができるのは電子メールのアドレスを持っている者とすると，発信者のメールアドレスが確認できる．電子メールは，送信に料金がかからないので経済的であるが，通常，電子メールには暗号がかからないので第三者が電子メールを盗み見ることが可能である．よって，鍵をそのまま電子メールを利用して送ることはできない．

次に考えられるものが，上記１と上記２の住

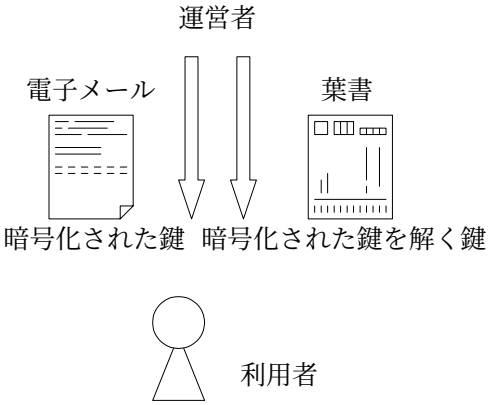

図２　住所氏名と電子メールアドレスを確認し安全に鍵を運ぶ提案手法

所氏名を使用した鍵の配布である．郵便物に書かれた鍵を読むことができるのは郵便物の送付先の住所氏名を持つ者とすると，発信者の住所氏名が確認できる．もっともコストのかからないものが，葉書である．葉書はメディア代を含めて５０円であるので，物理的な配送方法の中で，もっともコストが安い．しかし，葉書が完全に守られていない状態，例えば，郵便受けに半分入れられた状態や，鍵のかけられていない郵便受けに入れられた状態では，第三者が葉書を盗むことが可能である．よって，鍵をそのまま葉書として送ることはできない．

３．複数の異なるメディアを用いた発信者特定と安全な鍵送付方法

そこで，鍵をそのまま送るのではなく，暗号化を行い，暗号化された鍵を電子メールで送り，暗号化された鍵を解く鍵を葉書によって送る手法を提案する（図２）．鍵は暗号化されているので，上記３のメールアドレスとして登録された電子メールを盗聴することと，上記１と上記２の発信者の住所氏名宛に届いた葉書を盗むことを同時に行わなければ，鍵を復元することはできない．電子メールの盗聴と，葉書を盗む行為を同時に行うことは困難であるので，本提案手法を用いることで，送付した鍵を使用した情報発信者の氏名，住所，電子メールアドレスを特定することができる．

４．おわりに

本提案手法は，１人の発信者情報あたり５０円と，コストが安いので，零細企業であっても使用可能である．