「なりかわり」対抗可能な電子決済システムの提案

三輪信介† 篠田陽一†

本論文では，電子決済システムに対する新たな脅威を指摘し，この脅威に対抗可能な電子決済システムを提案する．安全なクレジットカード決済システム，電子現金，電子小切手など様々な電子決済システムが存在しており，これらのシステムでは，正しい支払いを行うためには，支払いに関する情報を正しい相手に伝達しなければならない．しかし，オープンネットワークシステム上では正しい相手をいつも指名できるとは限らない．そのため，相手を指名するとき（すなわち双方向認証が行われる前）に，不正者は自分を正しい受取人として指名させるための嘘の情報を与えることができ，正しい支払いを受けることができる．このような誤認は双方向認証を行う前に引き起こされるために，双方向認証によって正しい相手を認証する既存の電子決済システムでは防ぐことができない．この電子決済システムに対する新たな脅威を「なりかわり」と呼ぶ．本論文では，なりかわりの特性を明らかにし，この脅威に対抗するための電子決済システムへの2つの改善を提案するとともに，この改善を実装する．

"Pretense Resistant" Electronic Settlement System

SHINSUKE MIWA† and YOICHI SHINODA†

This paper proposes a "Pretense Resistant" Electronic Settlement System. Various Electronic Settlement Systems such as secure credit card payment systems, electronic caches and electronic checks do exist, and in order for a payment to be done correctly, these systems must communicate correct information about the payment with correct peers. However, on open network systems, the correct peer may not always be designated. That is, when designating a peer, before two-way authentication can take place, a malicious entity can give false information that can designate the entity as a payee. Notice that because the misdesignation occurs even before the two-way authentication is to take place, the existing Electronic Settlement Systems can not prevent this situation. This new type of threat to Electronic Settlement Systems is named "*Pretense*" in this paper. Characteristics of Pretense are explored, and two improvements for Electronic Settlement Systems to resist this threat are proposed and implemented.

1. はじめに

数多くの電子決済システムが提案/実装されており，多くのシステムがここ2，3年の間に実証実験段階に入った．これらのうちのいくつかは近年中に実用化されると目されている．また，インターネットのようなオープンネットワークシステム上での実現も同様に考えられており，今世紀中には実用化されるであろう．

現在の電子決済システムは，「誰が」「誰に」「いくら」という支払いに関する情報を支払人/受取人/決済機構の間で正しく伝達することで決済を行うシステムである．そのため，「盗聴」「改ざん」「なりすまし」などの様々なセキュリティ上の脅威にさらされるオープンネットワークシステム上の電子決済システムでは，情報を伝達する相手を特定するための双方向認証技術が重要な要素技術となる．

この双方向認証技術は，利用者が「正しい相手」を「指名」できることを前提としており，この指名に従って，「正しい相手」を「認証」する．しかし，オープンネットワークシステム上では，利用者が必ずしも正しい相手を指名できるとは限らないので，双方向認証技術によって正しい相手を認証できるとは限らない．そのため，「なりかわり」と呼ぶ新たなセキュリティ上の脅威が発生する[16]．

本論文では，この「なりかわり」が現状の電子決済システムでは解決困難であることを指摘し，この脅威に対抗するための電子決済システムへの2つの改善を示し，NECS方式[15]に対しこの改善を実装する．

† 北陸先端科学技術大学院大学情報科学研究科
The School of Information Science, Japan Advanced Institute of Science and Technology, Hokuriku

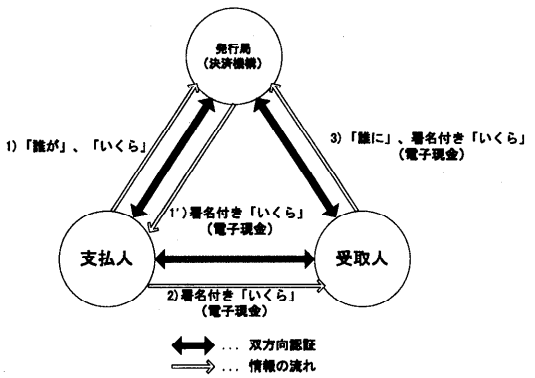


図1 電子現金の仕組み
Fig. 1 The outline of Electronic Cash.

2. 電子決済システムの概要

まず，電子決済システムの仕組みを概観してみよう．既存の電子決済システムのメカニズムはシステムによって様々であり，利用するメディアや決済の形態などに大きな違いがあるものの，どのシステムも「誰が」「誰に」「いくら」といった支払いに関する情報を，最終的な決済を行う機構に正しく伝達するシステムであるという点は同じである．

2.1 例：電子現金システムの仕組み

例として，電子現金システムのメカニズムについて概観してみる（**図1** 参照）[1),2),5),6),18)]．

電子現金システムのトランザクションは，以下の3つのステップに分けることができる．

(1) 利用者は，電子現金の発行を発行局（決済機構）に要求する．利用者は「誰が」「いくら」といった情報に署名し，発行局に送る．発行局は，この利用者からの要求に対し，「いくら」についての情報に署名し（発行局が証明した「いくら」についての情報，すなわち電子現金），利用者に送る．これらの利用者と発行局間の情報のやりとりの際には，双方向認証技術を使って互いに認証を行う．

(2) 利用者（支払人）は他の利用者（受取人）に電子現金を譲渡することで支払いを行う．支払人は，電子現金（発行局が署名した「いくら」についての情報）を受取人に送る．このとき，支払人と受取人は互いに認証する．

(3) 受取人は，決済機構（発行局）に電子現金の現金化を要求する．受取人は，「誰に」についての情報に署名し，電子現金（発行局が署名した「いくら」についての情報）とともに決済機構に送る．決済機構は，この受取人からの要求に対し，電子現金を検証し，現金化する．これらの受取人と決済機構間の情報のやりとりの際には，他のときと同様に互いに認証する．

実際の電子現金システムにおいては，匿名性の提供や分割機能の付加などのためにもう少し複雑であるが，概略は上述のとおりである．電子現金システムは，発行局→支払人→受取人→決済機構の順に双方向認証技術によって相互に認証しながら，署名済みの「いくら」についての情報を正しい相手に伝達していくことで，決済を行うシステムであるといえるだろう．

2.2 双方向認証技術

上述のように，電子決済システムは，「誰が」「誰に」「いくら」といった支払いに関する情報を，正しい相手に正しく伝達するシステムである．そのため，正しい相手を認証するための双方向認証技術は，オープンネットワークシステム上の電子決済システムにとっての重要な要素技術である．

付加価値網（VAN：Value Added Network）などのクローズドネットワークシステムや電子商取引市場（Electronic Marketplace）[19),20)]においては，ネットワークシステムや商取引市場そのものに双方向認証機能を付加することができるので，双方向認証技術は電子決済システムにとってそれほど重要な技術とはならない．

これに対し，インターネットのようなオープンネットワークシステムにおいては，通信路が不正者による「盗聴」「改ざん」「なりすまし」などの様々な攻撃にさらされるため，当然，電子決済システムもこれらの攻撃にさらされることになる．特に「なりすまし」は，電子決済システムにおいては，利用者に経済的損害を及ぼしうるので，防止されねばならない．そのため，「なりすまし」を防止することができる双方向認証技術は，このような環境においては非常に重要である．

双方向認証技術は，相手を認証するための技術である．そのため，電子決済システムにおいてこれを利用した場合，決済に関するプライバシーを露出する危険がある．そこで，プライバシーを保護するための技術が必要となる．この問題を解決するために，既存の多くの電子決済システムでは以下にあげた技術を応用している[10)]．

- ブラインド署名技術
- ゼロ知識証明技術
- 仮名に基づく検証技術
- 鍵寄託技術

しかし，プライバシーの保護は，同時に電子決済システムの犯罪への利用や資金浄財化（マネーロンダリ

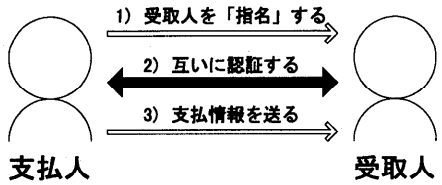


図2 電子決済システムにおける支払い
Fig. 2 The communication of payment on the ESS.

ング）を容易にする可能性がある．そのため，最新の電子決済システム[9)~12),15)]では，不正が検出されたときにプライバシーの保護を解除するために，より複雑なメカニズムを組み込んでいる．

3. 電子決済システムに対する新たな脅威

電子決済システムは，双方向認証技術と暗号技術，電子署名技術を組み合わて応用し，「盗聴」「改ざん」「なりすまし」などの既存のセキュリティ上の脅威を防ぐことができる．しかしながら，オープンネットワークシステム上の電子決済システムにおいて，「なりかわり」と呼ぶ新たな脅威が存在する[16)]．そこで，本章では，「なりかわり」の詳細について考察する．

3.1 正しい受取人の指名

オープンネットワークシステム上の電子決済システムにおいては，支払人は受取人に対して，以下のように支払いを行う．

(1) 支払人は受取人を「指名」する．
(2) 指名した受取人であるかどうか「認証」する．
(3) 支払いに関する情報を「伝達」する．

受取人は支払人を認証するので，一般に(2)は双方向認証である．このように，オープンネットワークシステム上の電子決済システムは，「指名」「認証」「伝達」から構成されていると考えられる（図**2** 参照）．

ここで，この「指名」が問題となる．なぜなら，オープンネットワークシステム上では，支払人が正しい受取人を指名できるとは限らないからである．もし，支払人が正しい受取人をすでに知っているのならば，支払人が間違った受取人を指名することはないだろう．しかし，もし支払人が正しい受取人を知らない場合，支払人はそもそも誰が本当に正しい受取人なのかを特定することができないので，正しい受取人を指名することは難しいだろう．

たとえば，支払人が受取人をIDによって指名する場合を考えてみよう．もし，すでに支払人が受取人とそのIDを知っているなら，そのIDで受取人を指名すればよい．また，未知の受取人を指名する場合でも，その受取人から正しいIDを受け取ることができたならば，問題は起こらない．しかし，受取人から受け取ったIDが途中で改ざんされていた場合，支払人は間違ったIDを受け取り，そのIDをその受取人のIDだと誤認してしまう．当然，支払人はそのIDが正しいと信じているので，そのIDを使って指名を行い，そのIDを持つ何者かに「正しく」支払いをしてしまう．これを利用して，正しい受取人のIDを自分のIDに改ざんすることで電子決済システム上は正しい受取人として支払いを受けることができる．

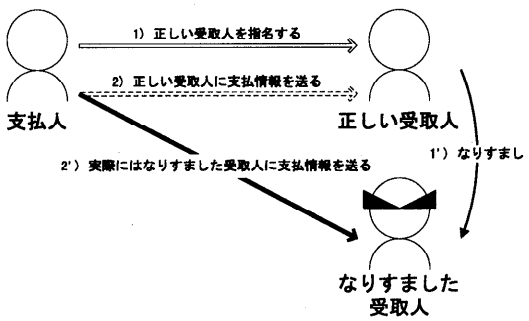


図3 「なりすまし」
Fig. 3 Impersonation.

こういった改ざんをオープンネットワークシステム上で防ぐためには，暗号化や電子署名，認証などによって安全に情報を提供することが考えられる．しかし，ネットワークシステム自身が安全性を提供しているわけではないオープンネットワークシステムにおいては，どこかの時点で相手を指名し，その指名した相手との間で安全に情報をやりとりすることしかできない．その指名そのものが間違っていた場合には，やはり問題を引き起こしてしまい，電子決済システムにおいてはその問題が経済的損害につながることになるだろう．

このように，オープンネットワークシステムにおいて，安全なやりとりをするための入り口ともいえる「指名」を利用した不正を「なりかわり」と呼ぶ．

3.2 「なりすまし」と「なりかわり」の違い

前述のように，正しい受取人を指名するための情報を改ざんすることで，不正に支払いを受けることが可能である．この不正を「なりすまし」と区別して，「なりかわり」と呼ぶことにする．ここで，「なりすまし」と「なりかわり」の違いについて考えてみよう．

図3 に「なりすまし」がどのように行われるのかを示す．「なりすまし」とは，

- 支払人は正しい受取人を指名する（1）．
- 不正者が正しい受取人に「なりすまし」する（1′）．
- 支払人はなりすました受取人に支払う（2′）．

といった行為である．支払人もしくは正しい受取人が

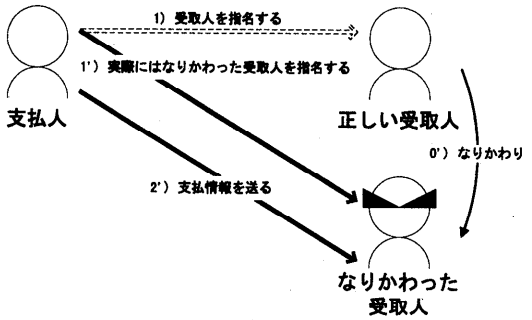


図4 「なりかわり」
Fig. 4 "Pretense".

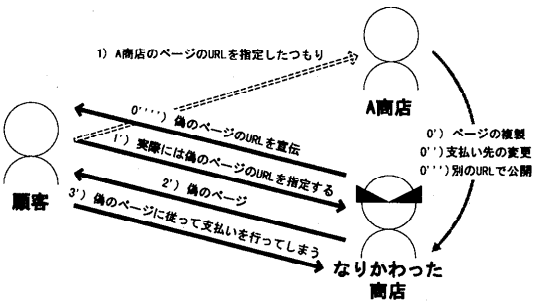


図5 「なりかわり」の具体例
Fig. 5 An example of "Pretense".

何らかの経済的損害を被るまで，この不正は検出されない．もし，支払人が受取人を正しく認証したならば，この不正を防ぐことができる．また，特定の受取人以外に利用できないように，支払いの情報に受取人を指名する情報が含まれていたならば，「なりすまし」によって正しい支払いを受けることはできない．

これに対し，「なりかわり」は「なりすまし」とは違い，以下のようなステップで行われる（図4参照）．

- 不正者は正しい受取人に「なりかわり」する（0′）．
- 支払人はなりかわった受取人を正しい受取人として指名する（1′）．
- 支払人はなりかわった受取人を正しい受取人として支払う（2′）．

もし，支払人がすでに正しい受取人について知っていた場合，支払人はなりかわった受取人が間違った受取人であることを知ることができるので，この不正を防ぐことができる．しかし，たとえ支払人が受取人を正しく認証したとしても，認証によってこの不正を防ぐことはできない．

3.3 「なりかわり」は可能か?

このような不正が本当に行いうるのかどうかについて，例として，インターネット上で電子商取引をする状況を考える．商品の提示や注文は，

- 電子メール
- World Wide Web

などを利用して行われると考えられる．ここでは，World Wide Web（以降Web）を利用する場合の「なりかわり」を考える．

Webを利用する場合，Webページを利用して商品情報の提供が行われ，フォームとCGIスクリプトなどを利用して注文が行われるのが一般的である．そして注文後，電子決済システムを利用して支払いを行う．このWebページには支払い対象を特定するための情報などが書き込まれており，この支払い対象をWebページ書き換え攻撃などで書き換えることで，「なりかわり」を果たすことが可能となる．しかし近年では，こういった攻撃に対する様々なセキュリティ対策がとられており，容易に書き換えることはできない．

しかし，「なりかわり」が脅威となりうるのは，こういったセキュリティ対策だけでは防ぎきることができないからである．以下にすでに知名度のある商店に対するなりかわりの例を示す（図5参照）．

> ある顧客がWebを利用した通信販売でネットワークカードを購入しようと考えたとする．彼は，A商店がWebを利用した通信販売でネットワークカードを販売していることを知っている．そこで彼は，A商店のWebページを探す．その結果，URLの違う2つのページが見つかる．双方のページともに内容は同じであるため，彼は疑いを抱かずどちらかのページでネットワークカードを注文し，電子決済システムを利用して支払いを行った．実はこのページがなりかわったページであり，結果，ネットワークカードはいつまでたっても送られてこない．A商店に直接問合せをしても「そのような注文はなく，支払いも受けていない」と言われるだけである．よって，彼は支払い分の損失を被ることになる．

これを行うのは容易である．「なりかわり」を行う者は，

(1) 有名な通信販売のWebページを複製する．
(2) 支払い対象に関する部分だけを自分宛てに変更する．
(3) 別のURLで公開する．

後は，このURLを適当なニュースグループやダイレクトEメールによって宣伝するか，登録型の検索エン

ジンへ登録するなどしておけばよい．このなりかわったURLを本物と間違えて，そのページで注文・支払いすると，その顧客は被害に遭うというわけである．これが簡単な「なりかわり」の方法である．

もっと端的な例としては，たとえば，ネットワークカードを販売しているように見えるWebページを作り，そのURLを適当に公表するという手がある．これは「ネットワークカードをWeb上で販売している商店」という抽象的なものになりかわっている例である．またもっと大掛かりな方法として，プリンストン大学のSIP（Secure Internet Programming）グループ[14]は虚像世界による攻撃（Mirror world attack）として，巧妙に偽のミラーサイトを作る手口を紹介している．

つまり，Webにおける「なりかわり」は，入り口となるURL自身に対して行われうるため，Webサイトおよびページを保護する様々なセキュリティ対策は意味をなさない．サイトの認証やページ作成者の認証が有効のように思えるが，Webを利用して電子商取引を行う場合，そもそもどのサイトにあるべきなのか，誰が作成者であるべきなのかが不明であるため，認証も意味をなさない．よって，このなりかわりは非常に単純ながら現状のセキュリティ対策では防ぐことができない．

3.4 「なりかわり」による脅威

電子決済システムにおける「なりかわり」とは，なりかわった受取人が正しい受取人として不正に支払いを受ける不正のことである．

既存の電子決済システムは，支払人が指名した受取人に正しく支払いをすることは保証するが，支払人が正しい受取人を指名したかどうかについては留意しない．言い換えるなら，電子決済システムにおいては，誰であろうと支払人が指名した相手が正しい受取人として扱われる．もし「なりかわり」が行われ，支払人がなりかわった受取人を指名すると，なりかわった受取人は電子決済システム上は正しい決済を受けることができる．これらのことから，既存の電子決済システムでは「なりかわり」を防ぐことはできないといえる．

では，支払いを行ってしまった後に，なりかわった受取人が正しい受取人ではないことに支払人が気づいた場合，支払いの返還要求が可能だろうか？ 本節では，このことについて考察する．

3.4.1 なりかわった受取人の特定

まずはじめに，受取人の特定について考えてみよう．支払人がなりかわった受取人が正しい受取人ではないことに気づいた場合，支払人は「誰に」支払ったのかを特定しなければならない．十分に安全でかつ匿名性を提供していない，安全なクレジットカード決済システムや電子小切手システムなどの電子決済システムにおいては，支払人は，システムの管理者と交渉し，受取人に関しての情報を得られれば「誰に」支払ったのかを特定することができるだろう．

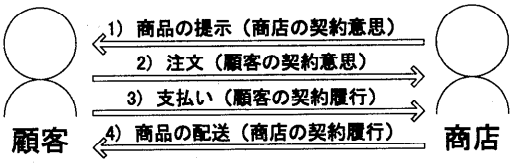


図6 一般的な通信販売における契約行為
Fig. 6 The contract of generic mail-order.

しかし，既存の電子現金システムの多くは，決済に関わるプライバシーを保護するために匿名性を提供している[2]．そのため，たとえ支払人がシステムの管理者と受取人に関する情報の提供について交渉し，了解を得たとしても，なりかわった受取人に関する情報は匿名化されており，入手することはできない．支払人が受取人の特定に必要な情報を入手することができなければ，当然，支払人はなりかわった受取人に対して支払いの返還を要求することはできない．

最新の電子決済システム[9)~12),15)]では，何らかの犯罪が行われた場合に犯罪者の決済に関するプライバシーの保護を解除することができる．こういった電子決済システムにおいては，支払人は受取人を特定することができる．

3.4.2 返還要求の法的根拠

次に，返還要求の法的根拠について考察する．仮になりかわった受取人を支払人が特定できた場合，支払人は間違った相手に対して支払いを行ったという事実を主張し，その事実を法的根拠に返還要求を行わなければならない．しかし，この返還要求の法的な根拠が存在するかどうかが問題となる．

一般に，支払いの返還要求の法的根拠は契約不履行である．例として，「通信販売でお金を支払ったのに商品が届かない」といった場合を考える．通信販売においては，一般に以下のような契約がある（**図6**参照）☆．

(1) 商品の提示（商店による契約意思の提示）
(2) 注文（顧客による商店の契約意思の確認と顧客

☆ 通信販売のように，社会通念として契約行為が明確な場合，明文化された契約は必要としない．実際，対面販売の場合には，契約行為が明確であるために，明文化された契約は存在しない．ただし，通信販売においては事後に起こるトラブルを避けるために，契約を明文化しておくのが一般的である．

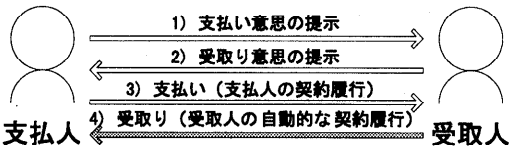


図7 電子決済システムにおける契約行為
Fig. 7 The contract of the ESS.

側の契約意思の提示）
(3) 支払い（顧客の契約履行）
(4) 商品の配送（商店の契約履行）

このような契約（売買契約）において，支払い（3：顧客の契約履行）を行ったにもかかわらず，商品の配送（4：商店の契約履行）が行われたかった場合，顧客は「契約の不履行」を根拠として支払いの返還を要求することができる．

しかし，現在の電子決済システムにおける契約行為は，こういった契約行為とは違う．以下に電子決済システムのトランザクションにおける契約を示す（図7）．
(1) 支払い意思の提示（支払人による契約意思の提示）
(2) 受取り意思の提示（受取人による支払人の契約意思の確認と受取人による契約意思の提示）
(3) 支払い（支払人の契約履行）
(4) 受取り（受取人の自動的な契約履行）

このような契約（支払契約）においては，たとえ支払い（3：支払人の契約履行）を行ったにもかかわらず，商品の配送がなされなかったとしても，受取り（4：受取人の契約履行）が行われていれば，契約の不履行とはならない．商品の配送は契約に含まれていないからである．

つまり，電子決済システム上では，「なりかわり」が行われた場合，なりかわった受取人が支払いを受け(4)，商品を送らなかったとしても契約不履行とはならない．そのため，「契約の不履行」を根拠として支払いの返還を要求することはできない．

これに対し，「電子決済システム上では売買契約を行っていないが，電子決済システムを利用して支払人が支払うに至るまでの過程で，何らかの売買契約を行っているはずだ」という抗弁が考えられる．しかし，支払人が支払いとその売買契約との結び付きを証明することができなければ，「契約の不履行」を証明することはできない．つまり，既存の電子決済システムは，売買契約をともなわない支払システムであるため，「契約の不履行」を根拠とする支払いの返還要求はできないといえる．

よって，電子決済システムにおいて「なりかわり」が行われた場合，支払人は受取人の「善意の返還」を期待するしかなく，受取人が「なりかわり」を故意に行っていた場合には，当然，返還される見込みはないと考えてよい☆．すなわち，「なりかわり」は，支払人に経済的損失をもたらし，なりかわった受取人への利益を生み出すことになる．

3.4.3 犯罪としての「なりかわり」

では次に，「なりかわり」を詐欺として取り締まることができないかを考える．「なりかわり」は明らかに詐欺行為である．しかし，「なりかわり」を詐欺として立件するためには，当然「なりかわり」が行われたという事実を証明しなければならない．

既存の電子決済システムは，「誰が」「誰に」「いくら」といった支払いに関する情報を正しい相手に正確に伝達するシステムである（2章参照）．そのため，当然ながら電子決済システムは，「誰が」「誰に」「いくら」といった支払いに関する情報以外，証明することはできない．言い換えるなら，電子決済システムは，「なりかわり」が行われたかどうかを証明することはできない．

もちろん，支払人が支払いに至るまでの過程をすべて証明可能な形で記録していたり，ネットワークシステムの管理者がやりとりされる情報のすべてを記録していた場合などは，「なりかわり」を証明することができるかもしれない．しかし，このような場合においても，現在の電子決済システム自身は無力である．

以上，本章で見てきたように，現在の電子決済システムでは「なりかわり」に対抗することはできない．しかし，「なりかわり」は十分可能な行為であり，経済的損害を利用者に与えうるため，今後電子決済システムが対抗しなければならない脅威であるといえる．

4. 電子決済システムの改善

現在の電子決済システムでは，安全ではない通信路を用いて受取人が自分を指名するための情報を支払人に通知する限り，電子決済システム自身が安全に設計されていたとしても，「なりかわり」を防ぐことはできない．そこで本章では，電子決済システムに対する，「なりかわり」に対抗するための2つの改善を提案し，NECS方式[15]に対し適用する．

「なりかわり」に対抗するための直接的かつ直観的な解決法は，
- 受取人を指名するための情報の公知

☆ 正確には，対価のない支払いが行われるとは社会通念上考えにくいので，まったく返還が行われないわけではないだろう．しかし，全額返還は望めないと考えてよい．

- 安全な通信路を用いた通信

が考えられる．しかし，オープンネットワークシステム上では，受取人が不特定であるため完全には防ぎきれない．そこで，電子決済システムに「なりかわり」に対抗するための以下の2つの改善を行うことを提案する．

- 追跡可能性の提供
- 契約機能の提供

以降では，これらの改善について詳細に議論する．

4.1 追跡可能性の提供

まず，電子決済システムにおいて，利用者の追跡を可能とすることを考える．追跡が可能となれば，たとえ「なりかわり」が行われたとしても，支払人は受取人を特定することができるので，もし有効な契約が存在すれば，その契約を基に返還を要求することが可能となる（3.4.1 項参照）．

もともと匿名性を提供しないような電子手形方式[8),13),22)]やクレジットカード方式[4),7),21)]では，追跡可能性はすでに提供されていると考えてよい．また，匿名性を提供しながら，プライバシーの保護を解除するためのメカニズムを組み込んだ電子決済システム[9),11),12),15)]についての研究が，ここ数年のうちにいくつかなされている[10)]．これらの方式は，不正が行われた場合，誰が不正を行ったのかを特定することができるので，追跡可能性を提供しているといえるだろう．

以上のように，電子決済システムに追跡可能性を付加し，なりかわった受取人を特定することは可能である．

4.2 契約機能の提供

3 章で見たように，仮に電子決済システムが追跡可能性を提供しているとしても，売買契約が存在しなければ返還要求をすることができない（3.4.2 項参照）．しかし，現在の電子決済システムは支払いしか取り扱わない．つまり，電子決済システムは支払人から受取人への支払いは取り扱うが，受取人から支払人への対価の支払いについては取り扱わない．そのため，「なりかわり」のような不正が可能となる．

そこで，「なりかわり」に対抗するために，返還要求の法的根拠となる売買契約を取り扱う電子決済システムを考える．

売買契約を取り扱えるように改善された電子決済システムのトランザクションは，以下の2つのステップに分けることができるだろう．

(1) 売買契約の締結
(2) 支払い

まず，ステップ (1) において，支払人は受取人との間で売買契約を締結する．次に，ステップ (2) において，支払人はこの契約に従い受取人に支払いを行う．この際，ステップ (1) で取得した情報をステップ (2) でのやりとりに織り込むようにする．このようにする理由は，「なりかわり」が行われた場合，支払人は売買契約と支払いの結び付きを証明しなければならないからである．

これにより，ステップ (1) とステップ (2) を分離することが可能となり，現金での決済と同様に後払いなどの様々な決済形態を実現することが可能となる．また，支払人は売買契約と支払いの結び付きを証明できるので，「なりかわり」が行われたとしても，売買契約の不履行を根拠として支払いの返還を要求することができる．

以上本章で見てきたように，現在の電子決済システムに「追跡可能性」と「契約機能」を付加することにより，「なりかわり」そのものを防ぐことはできないが，「なりかわり」にともなう損害を防ぎ，「なりかわり」に対抗することは可能となる．

5. NECS 方式の改善

前述のように，電子決済システムに対し「追跡可能性」と「契約機能」を付加することで「なりかわり」に対抗することが可能となる．そこで，本章ではインターネット上の電子決済システム NECS（Negotiable Electronic Currency System：裏書譲渡可能な電子銀行券システム）に対し，実際に「追跡可能性」と「契約機能」を付加することを考える．

NECS 方式[15)]は，インターネット上で最終的決済を行うことを目的として開発された，公開鍵暗号系を応用したインターネット上の電子決済システムで，オープンループ型の電子銀行券システムである．この方式では，利用者間の決済は，発行局など他の機関を介することなく，利用者同士で電子銀行券を譲渡することにより行うことができる．そのため，不正の検出は，「検証」や「引換」の際に発行局に電子銀行券が還流した時点で事後的に行われる．NECS 方式においては，利用者の決済に関する情報はすべて電子銀行券内に記録されるが，暗号化と仮名の利用によって匿名性が提供されている．

5.1 追跡可能性の提供

NECS 方式では，不正が検出された場合，PMA（仮名管理機構）は発行局に対し，不正者の実名を公開する．これにより，発行局は電子銀行券に記録されている決済情報と合わせて，不正に関する事実を証拠付きで示すことが可能となる．

これはすなわち，不正が発覚した場合に匿名性を解除し，決済を追跡することが可能であることを示しており，NECS方式はすでに追跡可能性を提供しているといえる．

5.2 契約機能の提供

前述のとおり，NECSは追跡可能性は提供している．しかしながら，契約機能は提供していない．そこで次に，契約機能を提供するためのNECSに対する改善を考える．

現在のNECSのトランザクションは，以下の4つである．

- 発行局から電子銀行券の振出を受ける「振出」
- 支払人から受取人へ電子銀行券を支払う「裏書譲渡」
- 電子銀行券に不正がないか確かめる「検証」
- 電子銀行券を現金化する「引換」

電子決済システムにおいて，契約機能を実現するために必要なことは，以下にあげたとおりである．

(1) 契約の締結
(2) 契約と支払いを結び付ける

そこで，売買契約を締結する（1）ための新たなトランザクションとして「契約締結」が必要となる．また，既存のトランザクションのうち変更が必要となるのは，利用者間での支払いに用いられる「裏書譲渡」である．「裏書譲渡」において契約と支払いを結び付ける（2）必要があるからである．

そこで，以降では「契約締結」と「裏書譲渡」のトランザクションについて考える．

5.2.1 「契約締結」トランザクションの追加

契約の締結は，安全に契約書をやりとりし，それに対して正しく互いに署名し，保管すればよいので，それほど複雑ではない．ただし，同じ契約文を利用することが多いであろうことを考えると，各契約書には個別のIDがつくことが望ましい．また，このIDは支払人もしくは受取人のどちらかが捏造できないように，互いの協調作業で作成されるようにする必要がある．

以上のようなことに留意し，作成したトランザクションを以下に簡単に示す．トランザクションにおいては，すでに互いに鍵の交換は済んでおり，すべての通信は相手の公開鍵で暗号化されているとする．$()^{SK_A}$ は，Aの秘密鍵による署名を示す．

(1) 支払人は乱数を生成し，署名して受取人に送る．
支払人→受取人：$(\text{支払人の乱数})^{SK_{\text{支払人}}}$
(2) 受取人は支払人が署名した乱数に署名し，乱数を生成し，署名して支払人に送る．
支払人←受取人：
$((\text{支払人の乱数})^{SK_{\text{支払人}}})^{SK_{\text{受取人}}}$,
$(\text{受取人の乱数})^{SK_{\text{受取人}}}$
(3) 支払人は受取人が生成して署名した乱数に署名し，契約IDを完成する．契約文とともに契約IDを受取人に送る．
契約ID：$((\text{支払人の乱数})^{SK_{\text{支払人}}})^{SK_{\text{受取人}}}$,
$((\text{受取人の乱数})^{SK_{\text{受取人}}})^{SK_{\text{支払人}}}$
支払人→受取人：契約文，契約 ID
(4) 受取人は受け取った契約文と契約ID（契約書）に署名し支払人に送る．
支払人←受取人：$(\text{契約文，契約 } ID)^{SK_{\text{受取人}}}$
(5) 支払人は受取人の署名のついた契約書を保管する．契約書に署名し，受取人に送る．
支払人→受取人：$(\text{契約文，契約 } ID)^{SK_{\text{支払人}}}$
(6) 受取人は支払人の署名のついた契約書を保管する．

このようにすれば，契約IDはどちらか一方で捏造することはできない．また，互いに相手が署名した契約書を持ち合うので，相手が契約をしていないと主張してもそれを退けることができる．

5.2.2 「裏書譲渡」トランザクションの変更

契約と支払いを結び付ける方法はいくつか考えられるが，支払いのトランザクションの内部で，契約書に対して，「支払い」という支払人の契約履行が行われたという事実を書き加える方法が単純であると考えられる．そこで，ある支払いを特定する情報とその支払いの内容を示す情報を，契約書に書き加えることにする．

さいわい，NECS方式では支払いの内容を示す情報は，「額面情報」として分離されており，また，ある支払いを特定する情報としては，裏書譲渡時に必ず生成され，記録される「セッションID」が存在する．そこで，これらの情報を然るべきタイミングで契約書に書き加え，互いに署名して交換するようにトランザクションを変更する．

ここで問題となるのは，交換するタイミングである．交換するタイミングが早すぎれば，契約書には契約履行の事実が記録されるが，実際には契約を履行しないことが可能となり，後に紛争が起こった場合には，支払人は契約書に契約履行の事実があることを根拠に，契約を履行したと主張することができてしまう．逆に，タイミングが遅すぎれば，支払いを行ったにもかかわらず，契約書には契約履行の事実が記録されないままになるということもありうる．

そこで，まず「裏書譲渡」のトランザクションをいくつかのステップに分割し，どの時点で契約書を交換

するかを考える．

(1) セッションIDの交換
(2) 受取人は領収書情報を支払人に送る
(3) 支払人は電子銀行券を受取人に送る
(4) 受取人は受取確認情報を支払人に送る

NECSにおいては，受取人が支払いを受けたにもかかわらず受けていないと主張することがないように，電子銀行券を送信する直前のステップで銀行券IDや銀行券番号とセッションIDを含んだ領収書情報を受取人に構成させ，送信させる．受取人が受け取っていないと主張した場合には，このステップから何度でもやり直せば，正しく電子銀行券を渡すことが可能である．

なぜなら，そのセッションにおいてその特定の電子銀行券を受け取ることができるのは，その領収書情報を示せる受取人だけであり，そのトランザクションを正しく行うことができるということは，すなわち正しい受取人であるからである．また，同じ電子銀行券を複数枚持っていたとしても，それを使えるのは1度のみであり，複数回使用すれば当然複製使用したと見なされ，不正者として扱われることになるからである．

さて，どの時点で契約書を交換するかであるが，(2)では支払いが完了していないので早すぎ，(3)では支払いが完了してしまうので遅すぎる．そこで，契約書に記録する内容を分け，1段階目では支払いを行っている最中であることが証明できるようにし，2段階目では支払いが終了したことを証明できるようにする．このようにすることで，たとえ支払いの終了を示す契約書が成立していなくとも，契約履行が行われている最中であったことを示すことができるので，その時点からやり直せば，契約を履行できることを証明できるはずである．

そうだとすると，自ずから1段階目を行うのは，やり直しを行うことができるところ，すなわち「領収書情報を送信する」(2)となる．第2段階目を行うのは，実際に電子銀行券を送るとき(3)とその確認をするとき(4)である．

以上のことをふまえて，領収書情報の送信のときからのトランザクションにおける契約書のやりとりを以下に示す．

(1) 受取人は銀行券IDと銀行券番号に発行局の署名がなされたもの(額面情報の一部)とセッションIDと支払人の署名がついた契約書に署名し(ある銀行券をあるセッションでこの契約の履行のためにやりとりしたことを受取人が証明する情報)，支払人に送る．

支払人←受取人：
$((\text{銀行券}\ ID, \text{銀行券番号})^{SK_{\text{発行局}}},$
$\text{セッション}\ ID, (\text{契約書})^{SK_{\text{支払人}}})^{SK_{\text{受取人}}}$

(2) 支払人は受取人の署名がついた新たな契約書を保管する．発行局の署名がついた額面情報とセッションIDと受取人の署名がついた元の契約書に署名し(ある額面の銀行券をあるセッションでこの契約の履行のためにやりとりしたことを支払人が証明する情報)，受取人に送る．

支払人→受取人：
$((\text{額面情報})^{SK_{\text{発行局}}}, \text{セッション}\ ID,$
$(\text{契約書})^{SK_{\text{受取人}}})^{SK_{\text{支払人}}}$

(3) 受取人は支払人の署名がついた新たな契約書を保管する．発行局の署名がついた額面情報とセッションIDと支払人の署名がついた元の契約書に署名し(ある額面の銀行券をあるセッションでこの契約の履行のためにやりとりしたことを受取人が証明する情報)，支払人に送る．

支払人←受取人：
$((\text{額面情報})^{SK_{\text{発行局}}}, \text{セッション}\ ID,$
$(\text{契約書})^{SK_{\text{支払人}}})^{SK_{\text{受取人}}}$

(4) 支払人は受取人の署名がついた新たな契約書を保管する．

このような変更をすることで，契約と支払いを結び付けることが可能となる．

以上のように，NECS方式に変更を加えることで，NECSを「なりかわり」に対抗できる電子決済システムとすることができた．

6. 今後の課題

今後の課題として，

- 実際に使う契約文をどうするか?
- 国際的に行われる遠隔地契約について

といったことを考えねばならない．

前者は，改善したNECS方式などで用いる契約文をどのようにすれば，トランザクションの様々な局面で問題が生じたとしても対応できるような契約になるかなどについてであり，いわば実運用時に必要な契約の雛形をどう作るかということである．

後者は，インターネットのような国と国とにまたがるネットワークシステムの上で遠隔地契約を結ぶ場合，国ごとに違う遠隔地契約に関する法律をどのように扱うかという問題である．これらについては，すでにEDIなどの分野で研究がなされており，それらの分野

で得られた成果を適用し，さらなる改善を図る必要があると考える[3]．

7. おわりに

本論文では，「なりかわり」という現在の電子決済システムが曝されうる新しい脅威を指摘した（3章）．また，技術的な特徴や法的な特性を示し，既存の電子決済システムが「なりかわり」に対抗できないと結論づけた．そのうえで，電子決済システムへの2つの改善（追跡可能性，契約機能）を示し（4章），既存の方式（NECS）へ実際に適用し改善を行った（5章）．これらの改善により，電子決済システムを「なりかわり」に対抗できるようにすることができることを示した．

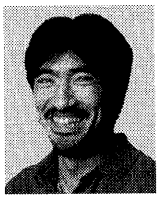
参考文献

1) Camenish, J., Piveteau, J.M. and Stadler, M.: An Efficient Fair Payment System, *Proc. 3rd ACM Conference on Computer Communications Security*, ACM (1996).
2) Chaum, D., Fiat, A. and Naor, N.: Untraceable electronic cash, *Proc. Crypto '88* (1988).
3) Clinton, W.J. and Gore, Jr. A.: A Framework For Global Electronic Commerce. ⟨URL: http://www.iitf.nist.gov/eleccomm/ecomm.htm⟩.
4) CyberCash, Inc.: CyberCash Home Page. ⟨URL: http://www.cybercash.com/⟩.
5) DigiCash, Inc.: DigiCash home page. ⟨URL: http://www.digicash.com/⟩.
6) Even, S., Goldreich, O. and Yacobi, Y.: Electronic Wallet, *Proc. Crypto '83* (1983).
7) First Virtual Holdings, Inc.: First Virtual Homepage. ⟨URL: http://www.firstvirtual.com/⟩.
8) FSTC: FSTC Electronic Check Project. ⟨URL:http://www.fstc.org/projects/echeck/index.html⟩.
9) Fujiaki, E. and Okamoto, T.: Practical Escrow Cash Systems, *ISEC 95-46* (1996).
10) 満保雅浩，岡本栄司：暗号最新事情9—供託電子マネー方式，*bit*, Vol.28, No.9, pp.101–109 (1996).
11) 三輪信介：インターネット上での通貨に関する研究，修士論文，北陸先端科学技術大学院大学情報科学研究科 (1997).
12) 三輪信介：インターネット上の譲渡可能な通貨システムに関する提案，情報処理学会研究報告，97-DPS-82, No.32, 情報処理学会 (1997).
13) 三輪信介，篠田陽一：インターネットを利用した手形決済システムの一提案，情報処理学会 DiCoMo ワークショップ 97-DiCoMo，No.30, 情報処理学会 (1997).
14) Secure Internet Programming Lab.: Secure Internet Programming. ⟨URL:http://www.cs.princeton.edu/sip/⟩.
15) Miwa, S. and Shinoda, Y.: The Negotiable Electronic Currency System on the Internet, *Internet Workshop '98 (IWS'98)*, *Proc. International Workshop on Asia-Pacific area advanced research information sharing technology*, IEICE (1998).
16) Miwa, S. and Shinoda, Y.: Pretense: A New Threat to Electronic Settlement Systems, *INET'98*, ISOC (1998).
17) Mondex International Limited: Mondex International. ⟨URL: http://www.mondex.com/index.html⟩
18) Okamoto, T. and Ohta, K.: Universal electronic cash, *Proc. Crypto '91* (1991).
19) Open Market, Inc.: Open Market Software Products. ⟨URL: http://openmarket.com/products/⟩
20) Open Trading Protocol Consortium: Open Trading Protocol. ⟨URL: http://www.otp.org:8080/⟩.
21) VISA and MasterCard: *Secure Electronic Transaction (SET) Specification Ver.1* (1997).
22) USC/ISI's GOST group: The NetCheque network payment system. ⟨URL:http://nii-server.isi.edu/info/NetCheque/⟩.

(平成10年 5 月 6 日受付)
(平成10年11月 9 日採録)

三輪 信介

1995年金沢大学経済学部経済学科卒業．1997年北陸先端科学技術大学院大学情報科学研究科修士課程修了．現在，同博士後期課程在学中．ネットワークセキュリティ，電子決済等を主に研究．日本ソフトウェア科学会学生会員．



篠田 陽一

1983年東京工業大学工学部卒業．1988年同大学工学部工学科助手．1991年より北陸先端科学技術大学院大学情報科学研究科助教授．工学博士．分散ネットワークシステム等の研究に従事．日本ソフトウェア科学会，ACM各会員．