전자상거래의 전자지불 기술

한국전자통신연구원 임신영 · 조현규 · 함호상
고려대학교 김태윤[*]

1. 서 론

전자상거래 전자지불기술의 구성은 하부기술로 시스템 통합 기술, IC 카드 기술, 암호화 기술 및 유무선 전산망 기술 등이 있으며, 응용기술로 지불 프로토콜 기술 및 전자화폐 단위 기술(발권, 양도, 분할, 위조식별 등)로 대별할 수 있다. 본 논문에서는 전자지불기술의 하부기술은 논외로 한다. 전자지불 기술이란 기존의 현금 및 수표 등의 지불 방식과 은행 계좌이체 및 신용카드 결제 방식을 컴퓨터 및 통신 기술을 이용하여 처리하는 기술로 크게 전자화폐 기술과 전자결제 기술로 대별되며 각각 온라인 및 오프라인에 대한 기술로 세분화 될 수 있다 특히, 전자화폐 기술은 다양한 전자 미디어(예: 스마트 카드, 무선 단말기, 휴대폰 등)에 적용할 수 있어 향후 이 분야의 기술 시장 형성 및 신규 서비스 제공이 예상된다.

대부분의 과정을 네트워크상에서 수행하는 전자상거래의 본격적인 전개를 위해서는 이용자의 부담을 줄이면서 안전하고 또한 저렴한 전자결제 시스템을 만드는 것이 필수 불가결한 조건이며, 이러한 전자결제시스템의 지불 수단으로서 전자화폐가 요구되고있다. 전자상거래 전자지불의 안전성을 제공하기 위한 방안으로 CGI나 자바 등을 이용한 인터액티브 결제 방식에 정보보호 기술과 프로토콜 표준을 적용하려 하였으나 기술제시 및 표준화의 문제로 지연되고 있다. 이를 극복하기 위한 다양한 기술적 대안들을 중심으로 본 논문을 구성하였으며, 이러한 전자지불 기술 체계 및 현재의 기술적 문제점과 향후 발전방향을 제시한다.

[*] 종신회원

2. 전자화폐 요구사항

2.1 전자화폐의 기본 요구사항

전자화폐는 일반적으로 물리적 화폐와 비슷한 기능을 제공하는 것이 기본적으로 요구되지만 완벽하게 물리적 화폐와 같은 기능을 갖는 전자화폐 기술을 구현하기는 몇 가지 제약이 있다. 그것은 물리적 화폐의 다양한 기능성을 전자화폐에 적용하기 위한 수학적 방식의 수용이 기술적으로 어렵기 때문이다. 한편 기존의 물리적 화폐는 다음과 같은 문제점을 가지고 있기 때문에 전자화폐의 구현을 위한 기술적인 문제 해결을 통하여 전자화폐를 실용화 하려고 노력하고 있다.

- 물리적 화폐의 제작, 유통, 관리 및 폐기에 인력과 비용 소요(신권 발권에 연간 약 4천억원)
- 컬러 복사기 및 프린터의 발달로 위조 화폐 제작 용이
- 급속한 컴퓨터 네트워크의 발전에 따른 전자상거래 시대에 온라인 결제 수단으로 기존 화폐 체계를 수용하기 어려움

위의 문제를 해결하기 위한 기술적 대안으로 전자화폐가 물리적 화폐의 특성을 완벽하게 제공하지 못함에도 불구하고 기술의 연구개발이 진행되고 있는 것이다. 전자화폐의 요구사항은 전자화폐의 기본적인 특징이 되며 이러한 요구사항은 다음과 같다.

• 안전성(security): 전자화폐의 안전성 정의는 여러 학자들에 의해 크게 두 가지로 대별되며 본 논문에서는 다음과 같은 두 가지 관점으로 분류한다.

① 물리적 안전성(physical security): 물리적 안전성이란 전자화폐 자체에 대한 위조의 어려움을 의미하는 것으로서, 전자화폐가 쉽게 위조될 수 없어야 한다는 것을 의미한다. 일반적으로 전자화폐는 스마트 카드라는 물리적 보안장치에 저장되는 것을 원칙으로 하기 때문에 결국 물리적 안전성이라는 것은 스마트 카드의 안전성으로 귀결된다.

② 논리적 안전성(logical security): 논리적 안전성이란 전자화폐 자체에 대한 위조 여부를 의미하는 것이 아니라 전자화폐 시스템의 각 구성원은 나머지 다른 구성원들의 공모 공격(collusion attack)에 대해 안전해야 함을 의미하는 것이다.

즉, 전자화폐의 안전성은 일반적으로 논리적 안전성을 의미하는 것으로 해석할 수 있을 것이다. 물리적 안전성이라는 것은 전자화폐의 안전성이라고 하기 보다는 IC 카드 자체의 안전성을 의미하기 때문이다. 본 논문에서는 전자화폐의 안전성 요구사항을 논리적 안전성으로 간주한다.

• 이중사용(double-spending) 방지: 전자화폐는 그 자체가 가치(Value)를 가진 디지털 정보이다. 디지털 정보는 종이 문서와는 달리 복사본의 생성이 용이하기 때문에 원본 및 사본의 구별이 불가능하게 된다. 결국 이중사용의 의미는 악의(惡意)의 사용자가 전자화폐를 불법 복제하여 반복적으로 사용하는 것을 의미하는 것이며, 이것은 전자화폐 설계 시 가장 중요하게 고려해야 될 부분이다. 이중사용 문제에 대한 해결방법으로는 다음과 같은 두 가지 방법이 존재한다.

① 사후검출(after the fact): 사후검출이란 사용자가 전자화폐를 발급 받을 때 금융기관이 전자화폐 내에 사용자의 ID 정보를 입력한 후, 사용자가 전자화폐를 이중 사용하는 경우, 사후에 금융기관은 이것을 감지하여 전자화폐 내에 삽입되어 있는 사용자의 ID를 추출하여 이중사용자를 추적하는 방법을 의미한다. 은행은 정당한 사용자(전자화폐를 단지 한 번만 사용한 자)의 전자화폐로부터는 사용자 ID를 추출할 수 없게 된다. 사후검출 방식은 많은 오버헤드를 가지게 된다. 이중 사용자를 사후에 검출해야 하기 때문에 기존에 사용된 전자화폐에 대한 데이터베이스를 유지시켜야 하며, 또한 범죄가 발생한 이후에만 해결 가능한 방식이 되기 때문에 이중사용 행위를 사전에 막을 수 없다는 문제가 있다.

② 사전검출(before the fact): Chaum 등은 처음으로 사전 검출 방법을 제안하였다. 사전검출의 기본 개념은 스마트 카드를 이용하여 사용자가 전자화폐를 이중 사용하는 경우, 같은 정보가 반복적으로 이용되는 것을 감지함과 동시에 작동을 중지시키는 방법을 취하는 것이다. 이것은 사후검출 방식의 문제점을 해결함과 동시에 전자화폐 시스템의 실질적인 구현에 발판을 마련하는 계기가 되었다. 현재 온라인 방식의 전자화폐는 기본적으로 사전검출이 적용된다. 즉, 예치 단계에서 은행이 개입하게 되어 판매자가 전자화폐를 은행에 예치하는 경우, 은행은 기존에 사용된 전자화폐의 저장 정보와의 동일 여부를 비교하여 이중사용을 사전에 검출할 수 있는 것이다. 그러므로 온라인 전자화폐는 전자화폐의 이중사용 문제를 해결하였다고 볼 수 있다.

• 프라이버시 (privacy): 전자화폐 기술과 지불 브로커 기술간의 차이는 사용자 프라이버시의 보장이다. 즉, 전자화폐는 실제 현금과 같이 사용자의 거래 내역이 추적되지 않는다. 이러한 사용자 거래의 불추적성을 일반적으로 사용자의 프라이버시라고 하며 사용자 프라이버시의 보장은 전자화폐의 가장 큰 장점이 되며, 프라이버시 보장 수준에 따라 다음과 같이 두 가지로 나뉜다.

① 불추적성(untraceability): 은행과 판매자가 어떠한 공모를 행하더라도 전자화폐를 지불한 사용자의 지불정보와 인출정보는 서로 연결될 수 없는 것을 의미한다. 즉, 은행은 판매자와 공모하더라도 사용자의 지불 내역을 추적할 수 없게 된다(물론 사용자가 단골 고객인 경우 판매자의 설명으로 은행이 지불자의 정보를 알 수는 있지만

후에 이것을 증명할 수는 없기 때문에 거래 내역에 대한 정보로서 사용할 수가 없게 된다).

② 불연계성(unlinkability): 은행과 판매자가 공모하는 경우 은행은 비록 사용자의 거래 내역을 추적할 수는 없지만 두 가지의 지불이 같은 사용자에 의한 것임을 알 수 있는 경우가 있는데(이것은 전자화폐의 설계 스킴에 따라 존재하며, 대표적인 예로는 전자면허를 사용하는 전자화폐가 있으며, 이는 불연관성 조건을 만족시키지 못하고 있다) 이러한 경우 연계성(linkability)이 있다고 본다. 이러한 연계성이 전자화폐에 존재할 경우 궁극적으로는 사용자의 불추적성이 보장되지 않을 수도 있게 된다. 그러므로 전자화폐가 완벽하게 사용자의 프라이버시를 보장하기 위해서는 불연계성이 보장되어야만 한다.

위와 같이 프라이버시는 그 수준에 따라 두 가지로 나뉘어지는데 일반적으로 ②의 조건을 만족하게 되면, ①의 조건은 당연히 만족되어지며, 보통 전자화폐의 프라이버시라고 언급되는 것은 대부분이 ②의 불연계성을 의미하는 것이다.

- 오프라인(off-line) 전자화폐의 요구사항: 전자화폐는 온라인 방식과 오프라인 방식으로 대별될 수 있다. 온라인 전자화폐는 사용자와 판매자의 거래 시 은행의 개입이 필요한 시스템으로 사용자가 판매자에 전자화폐를 지불하는 경우 네트워크 상으로 은행의 개입이 있어야 한다는 것이다. 반대로 오프라인 전자화폐는 사용자와 판매자의 거래 시 은행의 개입이 필요치 않은 것이다. 일반적으로 전자화폐는 오프라인 방식을 채택하고 있는데, 이것은 물리적 화폐의 기본 성질에 따른 것이며 컴퓨터 네트워크를 통해서 뿐만 아니라 일반 상점의 오프라인 단말기를 통해서도 거래를 보장하는 장점이 있기 때문이다. 다음 표 1은 온라인 방식과 오프라인 방식을 비교 설명한 것이다.

2.2 전자화폐의 부가 요구사항

전자화폐를 실제 화폐와 같이 사용하기 위해서는 다음과 같은 몇 가지 요구사항이 있다.

- 전자수표(electronic check): 최초의 오프라인 전자화폐 시스템인 CFN시스템은 잔액 처리 문제를 해결코자 전자수표라는 방식을 제안하였다. 이것은 사용자가 전자화폐를 발급 받는 경우, 금액이 큰 전자화폐를 발급 받은 후 사용할 때에는 자신이 지불할 금액만큼 만을 지불할 수 있는 형태이다. 이것은 잔액 처리의 문제를 해결해 줄 수 있으며, 더불어 상점에서 잔액을 위한 전자화폐를 별도로 마련치 않아도 된다는 장점이 있다. 그러나 인출·지불·예치 프로토콜 외에 또 다른 프로토콜을 필요로 하게 된다는 단점이 있다. 즉, 사용자는 발급 받은 전자수표를 사용한 후 발급 금액에서 지불 금액을 뺀 나머지 금액을 은행으로부터 상환 받기 위해서 상환 프로토콜(refund protocol)을 수행해야만 한다.
- 분할성(divisibility): 분할성은 전자수표와 비

표 1 온라인 및 오프라인 방식의 전자화폐 비교

구분	온라인(on-line) 방식	오프라인(off-line) 방식
방식	전자화폐의 지불단계와 결제단계를 동시 수행(지불 프로토콜과 예치 프로토콜이 실시간으로 수행)	수신된 전자화폐를 일괄 처리하여 은행에 결제를 요구하는 방식(지불 프로토콜 이후 예치 프로토콜 수행)
장점	지불단계와 결제단계가 거의 동시에 이루어지므로 이중사용을 지불단계 전에서 사전방지 가능(사전검출)	통신량 분산과 더불어 네트워크 인프라가 구축되지 않아도 사용가능
단점	통신량 집중화 현상과 통신량 증가에 따른 오버헤드 증가	이중사용이 일어난 후 은행에서 이중 사용자에게 대한 신분검출이 가능하므로 이중사용의 범죄 발생 가능
적용 분야	고액거래로 높은 안전성을 요구하면서 운용비에 대한 부담이 크게 작용하지 않는 현금시장에 적합	많은 양의 소액거래가 이루어지는 곳으로 이중사용으로 인한 부정 가능 금액이 소규모인 거래에 적합
주도국	미국(통신망의 발달)	유럽(스마트 카드의 발달)

슷한 개념으로서, 사용자가 전자화폐를 발급 받는 경우 발급 받은 전자화폐를 사용자 마음대로 나누어 사용할 수 있는 성질이다. 즉, 인출 받을 당시의 금액을 기준으로 사용한 총액이 지정된 금액을 넘지 않을 때까지 사용자가 나누어 사용할 수 있음을 말하는 것이다. 이것은 전자수표와는 달리 한 번 발급 받은 전자화폐를 여러 번 나누어 사용할 수 있으며, 또한 전자수표가 가지고 있던 상환 프로토콜(*refund protocol*)이 필요 없다는 장점을 갖는다. 그러나, 이것은 완벽한 프라이버시 보장을 할 수 없다는 단점을 가지게 된다. 즉, 불추적성은 만족하나, 불연계성은 만족되지 않는다는 것이며, 결국 분할성은 완벽한 프라이버시가 보장되지 않는다는 문제점을 가지고 있다.

• n회 사용가능성(n-spendability): 이것은 분할성의 개념과 비슷하지만 본질적으로는 큰 차이가 있다. 분할성은 사용자가 발행 받은 전자화폐 금액 내에서 사용자가 지불하기 원하는 금액만큼 사용금액에 맞추어 지불할 수 있는 기능이다. 반면에 n회 사용가능성은 금액을 나누어 사용한다는 개념보다는 지하철 정기권과 같이 동일한 금액을 횟수 기준으로 n번 까지 사용한다는 개념이다. 즉, n회 사용가능성은 어느 일정한 금액을 일정 횟수만큼만 사용 가능케 하는 것이다. 그러나, 이 기능도 분할성과 같이 불연계성을 만족시키지 못한다는 문제점이 생긴다.

• 양도성(transferability): 실제 화폐의 성질들 중 가장 특기할 만한 것은 쉽게 양도 가능하다는 것이다. 즉, 발행기관으로부터 만들어진 화폐는 그것의 수명이 다할 때까지 계속해서 사회에 유통된다. 그러나, 기본적인 요구 사항만을 만족하는 전자화폐는 그러한 양도 기능이 없으며, 이것은 전자화폐가 실제 화폐를 대치하지 못하고 있는 이유중의 하나가 된다. 이러한 문제점을 해결하고자, T. Okamoto 등은 양도성 기능을 갖는 전자화폐 시스템을 제안하였다. 그러나, 양도성 성질에는 두 가지 문제점이 존재하게 된다. 첫 번째는 사용자의 프라이버시가 보장되기 어렵다는 것이다. 즉, 양도 가능한 전자화폐가 이중 사용되었다고 가정할 경우, 은행은 이중사용자를 추적하기 위해서는 반드시 중간 양도자들에 대한 조사를 해야만 한다. 이 과정에서 부득이하게 이중 사용된 양도 가능한 전자화폐의 사용자들은 그들의 신분을 노출시킬 수밖에 없는 것이다. 두 번째 문제는 양도 가능한 전자화폐는 양도횟수가 증가할 수록 양도 내역에 대한 정보 크기가 증가한다는 것이다.

3. 전자화폐 기술

3.1 전자화폐의 분류

전자화폐는 화폐의 고유 기능을 제공하는 방법과 용도 등에 따라 여러 가지로 분류될 수 있다. 일반적으로 범용의 전자결제시스템은 실용 가능성과 방법 등의 차이에 따라 (1) 신용카드 결제의 발전형 방식, (2) PC 뱅킹 방식, (3) IC 카드형 전자지갑 방식, (4) 전자화폐 방식 등과 같이 4가지로 구분된다.

3.2 전자화폐(Electronic Cash) 시스템

전자화폐 시스템은 선불카드/직불카드를 응용하거나 순수한 전자화폐를 응용하는 시스템이다. 전자화폐 시스템을 구축할 수 있는 기술적인 요구조건은 상당히 진전됐지만, 현재 금융과 사회적 관습 그리고 통화량과 경제에 미치는 영향 등 사회·경제적인 관점에서는 아직 연구가 진행되지 않는 듯하다.

전자 수표나 신용카드 등의 전자결제 시스템이 실세계의 화폐에 그 기반을 두고 있는 것에 반해 전자화폐 시스템은 완전히 새로운 화폐의 발행을 목표로 한다. 실세계의 화폐와 사용방법을 동일하게 하기 위해 전자화폐가 갖추어야 할 특성은 익명성, 휴대가능성, 양방향성 등이 있을 수 있다. 즉, 전자화폐가 실세계의 현 규모와 같이 소액의 거래, 개인의 물품 구입이나 서비스에 적합한데 반해, 물건의 구입 또는 서비스를 받을 때마다 그 정보가 어딘가에 저장된다면 개인의 사생활이 침해될 수 있으며, 또한 이 정보가 악용될 수 있음을 의미한다. 이를 막기 위해서는 전자화폐의 익명성이 요구된다. 전자화폐 시스템은 사용자의 익명성 보장 문제와 함께 전자화폐의 중복 사용 문제, 즉 전자화폐의 불법적인 복사 문제 등을 해결해야 할 것이다. 다음은 국내외의 전자화폐와 관련된 현황을 소개한다. 그림 1은

전자화폐의 구조를 나타낸 개념도이다.

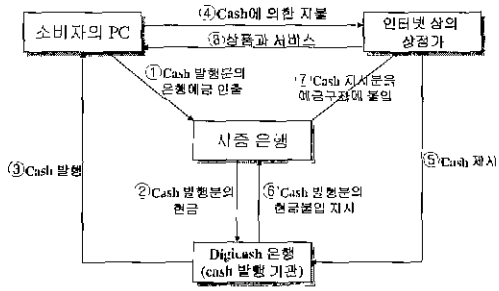


그림 1 전자화폐의 개념도

3.2.1 eCash

eCash는 네트워크상에 생성되는 가상 코인으로 DigiCash사가 개발하여 서비스하는 전자결제 시스템이다. DigiCash사는 네델란드에 본사가 있으며, 컴퓨터 암호기술에 관한 수많은 특허를 가지고 있다. eCash는 네트워크 상에서 지불행위를 하기 위한 전자화폐 개념으로서 소비자는 미리 은행구좌를 개설하여 자금을 입금해 두고, 전자메일과 전화 또는 편지 등으로 '민트(전자통화조폐국)'에 이체한다 전자 통화를 이용할 때에는 민트에게 이용자 PC로 전자 통화의 발행을 요구한다. 민트에서는 요구액에 상당하는 금액을 이용자 민트 잔고에서 끌어내어 이용자가 전자 통화를 이용할 수 있는 상태로 만든다. 이용자는 이 전자 통화를 이용하여 네트워크 상에서 지불을 하게 된다. 판매자는 받은 전자 통화를 민트에 송신하여 정당성을 체크한다. DigiCash에서는 민트라는 인증기능을 경유함으로써 전자 통화의 정당성을 확보하고 있다[1]. 이 기술은 중앙 집중적인 계좌 관리 때문에 거래의 많은 처리비용, 사용자 수의 제한 등의 단점이 있다.

3.2.2 NetCash

캘리포니아 대학에서 개발한 넷캐시(NetCash)는 복수의 서버(서버)를 도입하는 분산 시스템으로, DigiCash가 갖고 있는 중앙 집중적인 계좌 관리의 단점을 해결하려 하고 있다. 넷캐시는 DigiCash보다는 약한 익명성을 지원하고 있다. 그리고 사용자의 계좌를 분산된 여러 대의 서버에서 관리하며 사용자의 수를 극대화하는 데에 역점을 두고 있다. 또한, 넷체크(NetCheque)라는 전자 수표 시스템과 교환이 가능하도록 배려하고 있다.

1995년 제 4회 WWW 학회에서 Steve Glassman이 밀리센트 프로토콜(Milicent Protocol)이라는 아주 적은 액수의 지불에 사용하는 전자 지불 프로토콜을 제시했다[2]. 기본적으로 고객(customer)과 판매자(merchant)가 있으면 이 사이에 scrip이라고 부르는 전자화폐를 주고 받는데 이 서비스를 브로커(broker)라는 서버가 중간에서 중개한다는 기본적인 구조를 가지고 있다. 공개키 암호화 방식과 메시지 다이제스트 암호화를 혼용하여 정보보호를 제공하고 있는데, Glassman은 악의의 사용자가 scrip의 보안을 깨뜨리는데 드는 비용이 scrip의 지불 액수보다 커지도록 하면, 특별히 보안을 강화하지 않아도 적은 액수의 지불이 가능하다는 점에 착안하고 있다.

3.2.3 MONDEX

MONDEX는 Tamp와 resistant 특성을 갖는 IC카드 상에 현금가치를 이전하는 선불형 전자지갑으로서 영국의 내셔널 웨스트민스트 은행에서 고안된 전자결제 시스템이다[3]. MONDEX는 은행구좌에서 IC카드로 화폐가치를 옮겨 사용하는 방식으로 3.5초 정도면 현금처럼 결제할 수 있다. 특히, 크레디트 카드와 같이 거스름돈을 주고받는 번잡함이 없다. MONDEX의 실용화 실험은 웨스트민스트 은행과 미드랜드 은행이 공동출자로 세계 최초의 전자화폐 운영회사인 "MONDEX UK"를 설립, 인구 19만명의 영국 스윈던(Swindon) 지역에서 실용실험에 들어간 것이 최초이다. 영국 통신회사 BT가 개발한 공중전화를 사용하여, 사용자는 은행창구에 가지 않고도 돈을 MONDEX카드로 옮길 수 있게 되어 있다. BT는 가정용 전화기에도 동일한 기능을 제공하는 장치를 개발하였다.

이와 함께 현재는 인터넷을 매개로 화폐가치를 주고받는 메카니즘 개발에 주력하고 있으며, 일부는 좋은 결과를 도출하고 있다. 평상시에는 외부에서 쇼핑대금 지불에 MONDEX카드를 사용하고, 집에서는 인터넷을 통하여 전자결제에 쓸

수 있도록 하자는 것이 MONDEX의 목표이다.

MONDEX 카드는 IC의 위치나 치수, 이용하는 전압 등이 ISO에 근거하고 있으며, 현재의 실용화 실험은 홍콩, 미국, 캐나다의 주요은행을 통해 실시되고 있기도 하다. 또한, PC에 접속되는 카드리더는 미국 웰스파고 은행과 공동 연구중이다. 참고로 MONDEX는 1996년경 마스터카드 인터내셔널에 합병되었으며, 마스터카드는 MONDEX를 통하여 전자화폐 시장을 개척하고 있다.

3.2.4 Proton

Proton은 카드형 시스템으로서 선불(Prepaid) 체제이나 제 3자에게 가치이전을 할 수 없다는 점이 MONDEX와 다르다. 벨기에의 Proton은 1995년 2월부터 레우벤 등 2개 도시에서 시험을 개시했다. 이 카드는 소액결제 시장을 목표로 자동판매기 등에서 지불이 가능하도록 한 전자화폐 시스템이다. 시험서비스에 참가한 상점은 약 300개이고, 지불 단말 1,322대, 자동판매기 73대, 공중전화 50대 등이다. 그리고 소매점에서 취급대금의 0.7%, 자동판매기에서 2%를 수수료로 징수한다. 현재 Proton은 벨기에 국내에 3만매 이상의 카드를 발행하여 브뤼셀 등 대도시에서도 사용이 가능하다. 현재는 은행의 크레디트카드와는 별도로 발행하고 있으나, 일체화 계획으로 본격적인 "전자지갑"형태로 발전될 전망이다.

위의 4가지 대표적인 전자결제 시스템을 몇 가지 항목으로 비교한 표 2와 전자결제 수단별 특성을 표 3에 정리하였다.

표 2 전자결제 시스템 비교

	전자현금 시스템	전자수표 시스템	신용카드 시스템
적용범위	참가자간에만 가능	제한 없음	가맹점만
자금의 재사용	가능	가능	불가
은행을 경유하지 않는 기업, 개인간의 결제	가능	가능	불가
원격지로의 송금	은행을 경유하지 않고 가능	은행을 경유해야 가능	불가

표 3 전자결제 수단 비교

현 지불 수단	전자결제 수단		사례
현금	전자 현금	카드형	Mondex, 비자 Cash
		네트워크형	Ecash
수표	수표형		FSTC, Checkfree, Netcheck 사
신용카드	신용카드형		SET, CyberCash 사, First Virtual 사

4. 전자지불 기술의 문제점 및 해결 방안

향후 수년 이내에 전자상거래의 인프라가 인터넷이나 다른 네트워크 상에 구축될 것으로 예상된다. 전자상거래는 좋은 기회가 될 수도 있지만 한편으로 전대미문의 큰 위기일 수도 있다. 전자상거래 지불에 안전성을 보장하는 것은 매우 중요한 현안 사항이다. 그리고 전자화폐의 실용화를 위한 현안으로 전자화폐를 사회에서 용이하게 활용하는 방안과 이를 위해 해결해야 할 문제는 무엇인지를 파악하는 것이 중요하다고 할 수 있다. 또한 이러한 전반적인 방향이 경제에 어떤 영향을 미칠 것인지에 대하여도 신중한 검토가 있어야 겠다. 본 절에서는 전자화폐 및 전자지불의 실용화를 위한 몇 가지 문제점 및 일부 해결 방안에 대하여 검토한다.

4.1 위조 방지 문제

'0'과 '1'의 디지털 정보인 전자화폐는 디지털 데이터이기 때문에 쉽게 복사할 수 있다. 누구라도 플로피 디스크에 자기가 만든 문서를 복사하듯이, PC에 들어있는 전자 화폐를 복사하는 것은 위조지폐를 만드는 것과 동일하다. 전자화폐는 위조를 막기 위해 고도의 암호기술이 적용되고 있지만 완전한 암호는 아직 존재하지 않는다. 암호해독에 뛰어난 컴퓨터 해커가 전자 화폐를 위조할 염려는 없는지도 점검할 사항이다. 현재의 기술로는 전자 화폐에 사용되고 있는 암호를 해독하는데 슈퍼컴퓨터를 계속 가동해도 수년에서 수 십년이나 걸린다고 하지만 점차 연산에 소요되는 비용이 감소하기 때문에 안전하다고는 말할 수 없다. 컴퓨터 처리성능은 더욱 진보하고

있고 전자결제 시스템에 관계하는 당사자 중에 범죄의 유혹에 넘어가지 않는다는 보장도 없다. 결국 이러한 역기능을 방지하는 기술과 그것을 해독하는 측의 기술은 악순환 관계 또는 모순 관계를 유지하게 될 것이고 그 이상의 방지 기술을 안정적으로 운용하기 위한 사회 제도(법, 제도와 조직이용형태 등)의 검토가 무엇보다 중요하다고 말할 수 있을 것이다. 또한 암호화된 신용카드 결제에 대해서도 극히 간단한 방법으로 해독될 가능성이 있는 것이 실증되고 있느니 만큼 많은 연구가 필요하리라 본다.

4.2 국가 통화 관리 문제

국경을 넘는 인터넷에서 전자화폐의 흐름은 지금까지 국가를 근거로 발행되어 온 통화의 모습이 크게 바뀔 것을 쉽게 예상할 수 있다. 국내에 거주하고 있는 구매자가 인터넷을 사용해 온라인 쇼핑을 할 경우를 생각해 보자 접속한 상점은 호주에 있고, 이용자의 예금계좌는 싱가폴의 가상 은행, 상점 측은 카리브해의 작은 섬에 있는 은행에 거래계좌를 갖고 있으며 지불은 미화 달러와 연결된 전자화폐로 하고 물건은 인도의 업자에게서 보내져 올 수도 있다. 즉, 전자상거래가 본격화되는 시대에는 이런 복잡한 결제, 거래는 자연스러운 현상이 될 것이고 이를 위한 하부 기술의 지원과 함께 국가별로 관리하던 통화 관리 체계를 글로벌 개념으로 확대할 필요가 있다. 이를 위한 각국별 그리고 국제 통화 관리를 관장할 수 있는 국제 기구의 출연이 요구될 것으로 전망된다.

4.3 경제의 통제 불능 가속

네트워크내의 전자화폐에 의해 상거래의 속도는 가속될 것이고 통화량이 늘어나는 것과 똑같은 효과를 겪게 될 것이다. 문제는 1987년에 일어난 [Black Monday]같은 세계적인 시장의 대폭락이 다시 일어날 수 있는 위험도 높아지는 것은 아닌가 하는 것이다. Black Monday는 당시 도입되기 시작한 program trading의 폭주가 일으킨 사태이지만 전자화폐가 보급되고 네트워크를 통한 주식투자와 금융파생상품 등을 개인으로도 취급하는 것이 가능하게 되면, 국제경제 시스템의 제어불능에 박차를 가할 가능성이 충분히 있을 것이다. 실제 1995년에는 영국 증권회사의 젊은 사원이 금융파생상품의 실패로 거액의 손실을 내어 시장에 혼란을 주는 사태도 있었다

4.4 새로운 범죄 온상의 가능성

누가 사용했는가를 추적할 수 없고 자금의 흐름을 또한 추적할 수 없는 전자화폐는 사용방법에 따라서는 교묘한 범죄를 조장하는 수단이 될 수도 있다 마약판매 등 범죄 행위에 의해 얻은 자금을 복잡한 조작을 거쳐 깨끗한 돈으로 바꾸는 돈 세탁을 전자화폐 사용으로 간단히 할 수 있는 가능성이 있다. 국가가 전자 화폐의 흐름을 파악할 수 없으면 탈세도 횡행할 두려움이 있다. 지금으로서는 eCash는 은행계좌를 경유하지 않으면 현금으로 바꿀 수 없지만 전자화폐의 유통이 본격화되고 비합법의 자금을 취급하는 Black Market이 성립하지 않는다는 보장은 없다.

5. 결 론

2000년에는 전세계 1억대의 컴퓨터와 1백만개의 네트워크로 연결된 인터넷이 국가산업 정보화와 기업생산성 향상은 물론 향후 「산업사회」를 대체할 「정보사회」 구현에 그 초석이 될 것이라는 전망과 함께 사회 전 분야에 걸쳐 활용 가치가 점차 확대될 것이다. 이와 같은 현상은 국제연합 국제상거래법위원회(UNCITRAL)가 제정한 「전자상거래모델법」과 1998년 7월 독일에서 개최된 40개국 경제무역장관회의에서 채택된 「본 선언」을 계기로 전 세계로 확산되고 있다. 이는 정보가 부가가치를 증대시키는 중요한 자원으로서 그 가치는 정보의 공유와 상호연결의 범위가 확대될수록 더욱 커진다는 정보화 사회의 특징을 감안할 때 글로벌 네트워크인 인터넷의 활용이 정보화에 미치게 될 중요성을 용이하게 전망할 수 있다. 미국과 일본 등 주요 선진국들은 민간기업 컨소시엄을 중심으로 21세기 전략산업으로 전자상거래 기술개발과 국제표준화 활동의 조기 전개를 통해 인터넷 전자상거래 시장 선점을 위한 주도권 확보를 서두르고 있다. 인터넷 전자상거래는 동화상과 3차원 기법 등 다양한 멀티미디어 구현으로 기존 매체의 한 계를 극복할 전망이

다. 특히, 「커머스넷코리아」가 정부의 지원을 받아 추진하고 있는 「한국형 전자상거래 실험사업」이나 데이콤과 비자카드의 협력 등 민간 차원에서의 인프라 구축을 위한 시도가 활발히 전개되고 있어 전자상거래의 전망이 크게 기대된다. 특히, 전자상거래가 다양한 정보통신 환경에서 수행되기 위한 기술 표준 및 기술의 연구개발은 국가의 기술 인프라 구축 및 기술 시장 형성에 지대한 영향을 줄 것으로 보인다. 결국 인터넷상의 멀티미디어 기술의 획기적인 발전과 전자상거래 기반 구축을 위한 다양한 시도는 기존의 금융, 유통업무의 관행과 시장구조에도 많은 영향을 미쳐 유통망 중심의 시장구조가 소비자 중심으로 전환되는 생활패턴의 변화도 가져올 전망이다. 1995년 말부터 증가하기 시작한 대기업 및 공공부문에서의 인터넷 전자상거래에 대한 관심은 초고속망 또는 국가기간전산망 구축사업과 연계돼 급속히 증가하고 있으나 전자상거래 관련 표준화 및 핵심 요소기술 개발의 미비 등 취약한 국내 전자상거래 기술기반으로는 향후 전개될 「전자상거래 라운드」의 효과적인 대응이 어려울 것으로 전망되어 향후 이 분야에 대한 집중적인 문제 해결이 요망된다.

참고문헌

[1] www.digicash.com
[2] www.millicent.com
[3] www.mondex.com

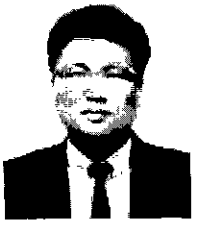
조 현 규

1980~1988 한국외국어대학교 독일어학과 문학사
1988~1990 고려대학교 대학원 경영학과 경영정보(MIS) 전공 석사
1993~1997 한남대학교 대학원 경영학과 경영정보(MIS) 전공 박사
1988~1990 현대해상 정보시스템부
1990~현재 한국전자통신연구원 전자상거래연구부 전지거래연구팀 팀장
관심분야 전자상거래 머천트 서버 기술, 전지지불 처리 기술, 개별화 서버 기술, 응용 컴포넌트 기술
E-mail hkcho@etri.re.kr

함 호 상

1977 고려대학교 산업공학과 졸업(B.S.)
1983 고려대학교 대학원 산업공학과 졸업(M.S.)
1995 고려대학교 대학원 산업공학과 졸업(Ph.D.)
1979~1981 대한지동차(주)
1982~1998 한국전자통신연구원 부설 시스템공학연구소 전지거래연구팀 팀장
1998~2000.2 한국전자통신연구원 전자상거래연구부 전지거래연구팀 팀장
2000.3~현재 한국전자통신연구원 전자상거래연구부 부장
관심분야 디렉토리 시스템 기술, 이동 에이전트 기술, 전자 지불 기술
E-mail:hsham@etri.re.kr

김 태 윤



1975~1981 고려대학교 산업공학과 학사
1981~1983 미국 Wayne State University 전산과학 석사
1983~1987 미국 Auburn University 전산과학 박사
1983~현재 고려대학교 컴퓨터학과 교수
1990~1993 정보통신부 및 정보통신진흥협회 자문위원
1990~현재 국립교육평가원 국가고시 출제위원
1992~현재 한국과학기술원 객원 책임연구원
1993~현재 한국통신 지문위원
1994~현재 총무부 국가고시 출제위원
1992~현재 APEC 통신실무 회의 국가대표
1998~현재 고려대학교 컴퓨터과학기술연구소 소장
관심분야 전자상거래, EDI, 인터넷 보안 전지 지불, 컴퓨터 그래픽스, 멀티미디어 통신
E-mail tykim@netlab.korea.ac.kr

임 신 영

1979~1983 건국대학교 공업화학과 학사
1983~1985 건국대학교 화학공학과 석사
1990~1992 건국대학교 전자계산학과 석사
1995~1998 고려대학교 컴퓨터학과 박사수료
1987~현재 한국전자통신연구원 전자상거래연구부 선임연구원
관심분야 인터넷 보안, 공개키 인증기관, 전자 지불, 디지털 콘텐츠 정보보호 기술
E-mail:sylim@econos.etri.re.kr