정보학연구 제2권 제2호 1999년 11월(pp.177-197)
The Studies of Information Technology, Vol.2, No.2

전자화폐의 유형별 도입 타당성 분석

서정교*

요 약

최근 전자화폐의 도입과 관련하여 여러 가지 정보 보안 기술상의 문제점들이 발생되고 있는 점을 중시하여 전자화폐의 유형별 안전성 평가를 통해 우리 나라에 있어서 전자화폐의 유형별 도입 타당성을 분석한다. 특히 암호기술의 선택조합이나 전자화폐에 대한 여러 가지 위·변조 유형을 고려하여 전자화폐의 안전성을 종합적이고 체계적으로 분석하며, 안전성은 뒤떨어지지만 화폐로서의 효율성과 기능성이 우월한 전자화폐의 경우에는 부정변조에 대한 내성장치(tamper resistance)와 같은 안전장치를 사용함으로써 그것이 중·장기적으로는 매우 유용한 전자화폐가 될 수 있음을 서술하고 있다.

Ⅰ. 서론

전자화폐의 도입 따른 여러 가지 문제점들이 노출되고 있는 시점에서 이에 대한 보안 대책이 다양한 이론적·실증적 측면에서 연구가 진행되고 있으며, 실제로 전자화폐가 기존의 화폐를 대체하여 일상생활에 보편적으로 사용되기 위해서는 예상되는 전자화폐의 보안 기술과 전자화폐의 유형별 도입 타당성 분석이 매우 중요한 의미를 갖는다고 하겠다. 특히 최근 전자상거래가 급속히 확산되고 있고 지불시스템 자체가 전자결제구조로의 전환을 요구받고 있는 시점에서, 전자화폐 도입을 위한 실험단계에 있는 우리 나라의 경우 여러 가지 유형 중 도입에 따른 위험을 최소화하고 보다 안전하게 유통될 수 있는 전자화폐를 개발하여 보급시키는 것이 전자금융시대의 새로운 과제로 부각되고 있다. 예컨대 IC카드형의 전자화폐의 대부분은 IC카드 내부의 정보를 부정한 방법으로 읽어내기 어려운 정도를 안전성의 근거로 하고 있는데, IC카드의 종류에 따라 부정변조에 대한 내성(tamper resistance)[1]의 강도는 다르기 때문에 실제로 필요한 수준의 보안 기능이 내장된 IC카드를 사용하는 것이 중요하다. 또한 사용하고 있는 암호 알고리즘(algorithm)의 선택 및 키 길이 설정, 키관리 등이 적절하게 이루어지고 있는가를 분석하는 것도 전자화폐 도입 타당성 분석에 직접적으로 영향을 주는 사항이다. 따라서 전자화폐의

* 중부대학교 경상학부 전임강사

1) 국제표준ISO 13491-1(Banking-Secure cryptographic devices(retail)-part1: Concepts, requirements and evaluation methods)에서는 안전한 암호 디바이스는 공격을 방지하는 부정변조에 대한 내성(tamper resistance) 이외에, 공격을 받았을 때 이것을 감지하여 반응작동을 하는 부정변조에 대한 반응성(tamper responsive), 공격을 받았을 때 그 증거를 기억하는 부정변조에 대한 증거성(tamper evident) 등의 특징을 가지는 것이 필요하다고 한다. 본고에서는 편의상 세 가지 경우를 총칭해서 '부정변조에 대한 내성'이라는 표현을 쓰고 있다.

유형별 보안 대책이 어떤 종류·정도의 위험을 갖춘 것인가를 충분히 파악한 상태에서 그 기술적 과제를 해결하기 위한 합당한 수준의 안전성을 충분히 분석하여 우리의 실정에 맞는 전자화폐를 단계적으로 도입해야 할 것이다. 따라서 전자화폐의 갑작스런 도입에 따른 역기능적인 충격(충돌착륙)을 피하고 21세기 새로운 결제시스템으로서 전자화폐의 연착륙을 실현하는 것은 매우 중요한 과제이다.

본고에서는 우선 제2장에서 전자화폐의 개발 실태와 과제를 검토한다. 다음으로 제3장에서는 전자화폐의 모델 유형을 분석하고 유형별 암호기술의 선택 방법에 대해서 살펴본 뒤, 제4장에서는 예상되는 여러 가지의 위험(위조) 요소를 고려하여 암호기술의 선택과 관련한 전자화폐의 모델 유형별 도입 타당성을 구체적으로 분석한다. 그리고 이러한 분석 결과는 각 전자화폐의 실현방식 간의 우열관계를 나타냄과 동시에 각각의 전자화폐 실현방식이 종합적인 안전성을 확보하기 위해서는 어떠한 요소기술(부정변조에 대한 내성 장치 등)을 추가할 필요가 있는가를 검토하는 자료로 이용할 수 있도록 한다. 마지막으로 제5장에서 이를 정리하여 결론에 갈음하고자 한다.

II. 전자화폐의 개발 실태와 도입 과제

2.1. 전자화폐의 개발 실태

전자화폐가 본격적으로 세계적인 관심사가 된 것은 1995년 영국의 소도시 스윈던(Swindon)에서 Mondex라는 전자화폐가 실험적으로 도입되면서부터이다. 그 이후에 세계 각국에서는 현재 여러 가지 유형의 전자화폐가 실험 중에 있거나 실용화 단계에 있다.

국제결제은행(BIS)에서 1998년 3월까지 파악된 각국의 전자화폐의 개발 실태를 살펴보면 휴대하기가 쉬운 IC카드형 전자화폐의 경우, 조사대상 75개국 중 36개국에서 76개 프로젝트가 진행 중에 있는 것으로 조사되었다. 전국적으로 운영 중이거나 확산 중인 국가는 오스트리아, 벨기에, 덴마크 등 13개국[2]이고 시험 운영 중인 국가는 영국, 미국, 일본 등 18개국[3]이다.

이들 IC카드형 전자화폐의 발행자는 주로 은행 또는 은행출자 전문회사이며, 비은행 발행자로는 카드기술회사, 운송 및 통신회사, 유통회사 등이 있다. 국내외 겸용을 목표로 추진 중인 프로젝트는 아직 없으나, VISA Cash, Mondex, Proton, CASH, Chipper, PMB, Avant 등이 현재 다른 나라에도 보급 중에 있다.

한편 컴퓨터를 통해 네트워크 상에서 가상의 화폐를 생성시켜 결제수단으로 활용하기 때문에 휴대하고 다니기가 불편한, 네트워크형 전자화폐의 경우는 네덜란드 DigiCash사가 개발한 E-cash와 미국 CyberCash사가 개발한 CyberCoin 두 종류만 현재 상용화 단계에 있으며, 많은 나라

2) 이들 국가들의 전자화폐 명칭은 다음과 같다. 오스트리아(Quick), 벨기에(Proton), 덴마크(Danmont), 핀란드(Avant, Matkahoulto), 독일(Geldkarte, Pay-Card, P-Card), 이태리(MINpay), 리투아니아(IMPAR), 네덜란드(Chipknip, Chipper), 포르투갈(PMB), 싱가폴(CashCard), 스페인(Monedero 4B, VISA Cash, Euro 6000), 스위스(CASH), 대만(FISC)

3) 구체적으로는 영국, 미국, 호주, 브라질, 캐나다, 콜롬비아, 체코, 코스타리카, 프랑스, 그리스, 홍콩, 이스라엘, 일본, 뉴질랜드, 노르웨이, 스웨덴, 태국, 터키 등이다.

들이 이 두 종류의 전자화폐를 도입하는 형태로 프로젝트를 진행 중에 있다.[4] IC카드형 전자화폐인 일본의 SuperCash와 영국의 Mondex는 현재 네트워크 겸용으로 추진 중에 있으며, 그 밖의 상당수의 IC카드형 전자화폐 프로젝트들이 카드 리더기(card reader) 등을 이용하여 네트워크 상에서도 사용할 수 있도록 하는 내용을 담고 있다. 네트워크형 전자화폐의 발행자는 대부분 은행이며, 비은행 발행자로는 통신회사, 전자쇼핑센터, 인터넷 운영자 등이 있다.

우리 나라의 경우는 1994년 3월 광주은행이 최초로 전자화폐 도입을 시도하였으나 개별은행 차원에서 시스템을 구축하였기 때문에 이용자 및 가맹점 확대에 실패하여 발급 및 사용실적이 부진하다. 곧이어 1995년 8월 당시 동남은행이 재정경제원으로부터 전자화폐 발행을 승인받아 「하나로 카드」라는 전자화폐를 발행한 적이 있다. 이것은 일반상점, 택시, 지하철, 전화 등에 사용하도록 설계되었으나 이용자 쌍방 간의 자금이체가 불가능하여 Mondex와는 차이가 있다. 그외에 최근 교통카드를 중심으로 IC카드형 전자화폐를 지방자치단체 차원에서 개발되어 실용화 단계에 있다. 그리고 한국은행과 22개 은행, 7개 카드사로 구성된 '금융정보화추진 은행 소위원회'는 1999년 10월을 전후해 여의도, 명동, 강남 또는 경주 등 몇 개의 대상지역 중 한 개 지역을 선정하여 시범사업을 벌이기로 한 바가 있다. 그러나 일반대중들의 전자화폐에 대한 인지도가 낮고 보안문제 등 전자화폐의 활성화에 많은 난제가 남아 있다(지호준, 1999).

4) E-cash는 호주, 오스트리아, 핀란드, 독일, 일본, 노르웨이, 미국 등 7개국에서 도입을 추진 중에 있으며, CyberCoin은 독일, 일본, 영국, 미국 등 4개국에서 도입을 추진 중에 있다.

2.2. 전자화폐의 도입 과제

전자화폐의 성공적인 도입과 발전에 장애가 되는 몇 가지 원인과 과제들이 존재한다. 특히 전자화폐의 보안 기술 문제는 각국의 공통된 과제로 부각되고 있다.[5]

본 장에서는 전자화폐의 도입 타당성 분석을 위해 우선 일반적인 보안사고의 유형에 대해서 살펴 보고 이러한 보안 사고를 방지하는 여러 가지 보안기술의 실태와 과제를 제시함으로써 안전하고 효율적인 전자화폐를 도입하기 위한 전제적 논의로 삼고자 한다.

전자상거래나 전자화폐의 유통과정에서 몇 가지 형태의 보안사고가 예상된다. 우선 오픈 네트워크 상에서 거래가 이루어질 경우 인터넷을 통해 악의의 제3자에게 송신자의 정보가 도중에 탈취당하여 원래의 정보가 변조될 위험이 있다. 둘째, 거래 당사자에 대한 본인 인증이 어려운 점을 이용하여 이용자 자신의 지불정보를 변조하거나 마치 특정인 또는 불특정인인 것처럼 위장하여 타인의 정보를 위조·이용하는 경우도 있다. 셋째로 상점이 고객과 결탁하여(결탁이 없는 경우도 있을 수 있음) 환류정보를 위조함으로써 은행으로부터 가치를 부정하게 이전시키는 경우가 있을 수 있다. 넷째로 오픈 네트워크를 통해 시스템에 침입하여 고객의 각종 정보 및 관리정보가 구축되어 있는 판매자의 서버나 은행의 컴퓨터를 해킹하는 경우이다. 이 때 이러한 정보들을 불법 유출 또는 변조하거나 시스템

5) 일전에 전자화폐 활성화의 장애요인에 대한 설문조사 결과에서도 '보안문제'가 4.09점으로 가장 높게 나타났으며, 다음은 '신뢰문제'가 3.77점, '인터넷 보급과 장치기비'가 3.72점, '가맹점의 미비'가 3.66점, '서비스 문제'가 3.60점, '전자화폐에 대한 이해의 난이성'이 3.45점의 순으로 나타났다(지호준, 1999).

자체를 파괴하게 되면 경우에 따라서는 매우 심각한 결과를 초래할 수도 있다. 이러한 경우 시스템 보호를 위해 반드시 방화벽(firewall)을 설치해 두어야 한다.

이와 같은 보안사고에 철저히 대응하지 못하면 인터넷에서의 전자상거래나 전자화폐는 아무 힘을 발휘할 수가 없게 된다. 따라서 보안사고의 유형에 맞는 적절한 보안대책이 마련되어야 한다. 이를 위해 여러 가지 암호기술이나 부정변조에 대한 내성 기술 등이 사용되고 있다. 현재 이용되고 있는 정보 보안기술에는 어떤 것들이 있는지 주요 요소기술을 살펴보면 다음과 같다.

2.2.1. 암호 기술의 과제

암호 알고리즘은 이용자에 대한 키의 배치방식에 따라 공통키방식과 공개키방식으로 구분된다. 특정의 수신자에게만 평문의 의미를 알 수 있게 하기 위해서는 복호화 키를 수신자만이 비밀로 가지고 있어야 한다. 암호화 키도 비밀로 해 두는 방식이 공통키 암호이고, 암호화 키는 복호화 키와 동일한 것이 일반적이다. 그러나 이 암호방식의 문제점은 암호해독을 위한 비밀키를 메시지 수신자에게 안전하게 전달하기가 어렵다는 것이다. 특히 인터넷과 같은 오픈 네트워크 환경에서는 전송 도중 도난당하거나 변조될 우려가 있다.

암호에 의한 보안장치에 있어서 암호화 키로부터 복호화 키를 유도해 내기 위해 막대한 계산량을 필요로 할 경우, 암호화 키를 공개해도 별 무리가 없다고 생각하여 이를 공개하는 방식이 공개키 암호이다. 특히 전자상거래나 전자결제시스템에서는 불특정 다수인과 거래하기 때문에 암호화에 필요한 비밀키를 일일이 거래 상대방에게 전달하는 것은 현실적으로 어렵기 때문에 이를 해결하기 위해 암호 키의 전달과정을 생략함으로써 암호화와 복호화에 각각 다른 키를 사용하고 그 중 하나를 공개하는 암호화 방식이 개발된 것이다. 암호에 의한 인증장치도 앞에서 설명한 보안장치와 원리가 매우 유사하다.

한편 공통키 암호에서 이용되는 키 길이는 알고리즘에 따라 다양하고, 가장 많이 보급되고 있는 DES(Data Encryption Standard)의 경우, 키 길이는 56비트이다. 이것은 키 길이가 짧아서 가능성이 있는 모든 키를 시험해 보는 全數探索에 의한 공격이 가능할 지도 모른다. 따라서 각국에서는 고도의 보안기술을 개발하여 암호화 키의 길이를 연장해 나가고 있다. 그러나 실용화되고 있는 공통키 암호에 있어서 128비트의 키도 언젠가는 해커들에 의해 위협을 받을 수도 있다. 즉 이용목적에 상응하는 충분한 키 길이를 가지는 것은 안전한 암호의 필요조건이지 충분조건은 아니라는 것이다(松本 勉 · 岩下直行, 1999).

추가적인 고려사항으로서 암호 알고리즘 자체가 충분히 강하다고 하더라도 암호키 관리가 문제가 될 수 있기 때문에 이에 대한 대책도 강구되지 않으면 안된다.

특히 전자화폐는 공개키 암호, 공통키 암호, 디지털 서명, 블라인드 서명(blind signature)[6], 해시함수(hash function)[7], 키배송 · 공유방식 등

6) 통신 내용의 일부를 비밀로 하고 디지털 서명을 붙여 받는 방식이며, 이 때 서명 요구자는 서명자에게 비밀문서의 내용을 모르게 하고 서명 요구자의 본인확인만 할 수 있게 한다.

7) 한 쪽으로의 연산에 비해 그 역방향으로의 연산이 대단히 어려운 일방향성 함수(one way function)로 이 함수의 연산결과는 고정된 크기의 데이터를 산출한다. 통상 인증방법에는 해쉬함수를 이용한 인증과 공개키 방식을 이용한 인증 두 가지가 있는데, 전자의 경우 A가 어떤 호스트에 접속하고자 할 때 우선 A가 호스트에 패스워드를 보내면 호스트는 패스워드에 해쉬함수를 적용하여 해쉬값을 구한 뒤, 이 값과 이전에 저장된 값(암호화

의 암호기술이 필요에 따라 서로 조합에 의해 실현되고 이들의 암호기술이 가지는 강도가 그대로 전자화폐 안전성의 수준에 영향을 준다. 또한, 컴퓨터의 기술진보나 새로운 공격법의 출현으로 종래 안전하다고 생각되었던 암호에 대해서도 그 안전성이 저하될 가능성도 있다. 따라서 신뢰할 수 있는 안전한 암호기술을 사용해 전자화폐를 구성할 필요가 있으며 아울러 항상 최신 기술동향을 살펴 안전성을 배려한 적절한 암호키의 길이나 유효기한의 설정 등에 각별한 노력이 요구되고 있다.[8]

2.2.2. 부정변조에 대한 내성 기술의 과제

부정변조에 대한 내성 기술이란 외부로부터의 부정한 방법 등에 의해 비밀정보를 관측·변조하거나, 본래의 설계 의도와는 다른 부정한 동작을 행하게 하는 것 등을 방지하기 위한 물리적·논리적 기술이다. 이같은 부정변조에 대한 내성 기술을 사용해 실현되는 것으로서는 CPU (Central Processing Unit)를 내장시킨 IC카드(스마트카드)가 대표적이다. IC카드는 내부정보에 접근하기 위해서는 정규 절차를 밟는 것이 필요하며, 외부로부터 직접 메모리에 접근해서 정보를 읽어내는 것이 곤란한 구조로 되어 있다. IC카드에는 외부단자가 부착된 접촉형 IC카드와 외부단자가 없는 비접촉형 IC카드가 있는데 현재 전자상거래 프로젝트 등에서는 주로 접촉형 IC카드가 사용되고 있다.

특히 IC카드의 부정변조에 대한 내성을 공격하기 위한 해석기술은 반도체제조·검사기술과 밀접한 관련이 있고, 많은 비용을 들여 반도체 제조·검사를 하는 최신장치를 이용한다면 공격이 가능하다는 견해이다.

IC카드의 공격방법은 주로 (a) 물리적 구조해석과 (b) 논리적 데이터 해석으로 나눌 수 있다. 물리적 구조해석은 외부 회로 등을 직접 관찰함으로써 IC칩의 구조나 거기에 기억되어 있는 데이터를 해석하는 방법이다. 관찰하기 위해서는 통상, 칩의 표면을 노출시키는 등의 물리적으로 손을 댈 필요가 있다. 한편, 논리적 데이터 해석이란, 정상일 때와 비정상일 때 IC회로의 동작 상황의 변화를 관찰함으로써 내부의 정보를 관측하는 해석방법이다. 의식적으로 고장을 일으켰을 때의 상태변화나 실전에 배치되었을 경우 처음으로 나타나는 암호처리의 특징을 이용해서 비밀정보를 빼내는 방법 등이 있다.[9]

그런데 전자화폐 등에 이용되고 있는 암호의 키나 거래 데이터 등이 폭로되지 않도록 또는 잔고 데이터 등이 변조되지 않도록 이들을 물리·논리적으로 엄중히 관리하는 것이 필요하다. 이를 위해 부정변조에 대한 내성을 가진 하드웨어나 소프트웨어 모듈, 즉 비밀 데이터를 외부에서 부당하게 관측·변조하거나 비밀 데이터의 利用制御部를 부당하게 변조하는 행위를 방지하는 하드웨어나 소프트웨어 모듈의 중요성이 커지고 있다. 전자화폐를 다루는 IC카드는 물론, IC카드를 집어넣는 장치, 전자화폐를 발행·관리하는 장치 혹은 인증기관의 증명서 발행장치 등에 부정변조 방지를 위한 내성 장치가

되지 않은 패스워드 대신에 패스워드의 해쉬값)과 비교하여 인증한다(구체적인 내용은 신일순(1996) 참조).

8) 각 암호방식의 강도에 대해서는 宇根·岡本(1999), 宇根·太田(1999) 외에 많은 문헌에서 논하고 있어 참조를 바란다.

9) 구체적으로는 (a) 전수탐색, (b) 고장이용공격(differential fault analysis 혹은 fault based attack) (c) 타이밍 공격(timing attack) (d) 전력차분공격(differential power analysis) 등이 있다. 자세한 내용은 中山 靑司·松本 勉·太田和夫(1999)를 참조하기 바란다.

필요하다. 암호장치의 부정변조에 대한 내성에 관해서는 현재 국제표준화기구(ISO) 등에서 기술평가가 진행 중에 있다(中山 靑司·松本 勉·太田和夫, 1999).

Ⅲ. 전자화폐의 모델 유형과 암호기술

3.1. 전자화폐의 모델 유형

3.1.1. 일반적 분류에 의한 유형

전자화폐는 통상 전자돈(electronic cash), 전자지갑(electronic wallet), 디지털 머니(digital money) 등 여러 가지 용어로 사용되고 있으나 내용 상으로 보면 다양한 유형의 전자화폐가 존재하여 개념 상 혼란을 야기시키고 있다. 따라서 우선 일반적 요인에 의해 분류기준을 단순화시켜 현재 실험 중에 있거나 실제로 통용되고 있는 각종 전자화폐를 유형화하여 분석하고자 한다.

전자화폐는 우선 휴대가능 여부에 따라 IC카드형 전자화폐와 네트워크형 전자화폐로 구분할 수 있다(제일금융연구원, 1997). IC카드형은 휴대가 간편하여 일반 화폐처럼 사용할 수 있는 반면, 네트워크형은 컴퓨터를 통해 네트워크 상에서 가상의 화폐를 생성시켜 결제수단으로 활용하기 때문에 휴대하고 다니기가 불편하다는 단점이 있다.

IC카드형은 중앙처리장치와 기억장치(memory) 등으로 구성된 극소형 마이크로 칩이 핵심부품으로 내장되어 있어서, 모든 정보가 CPU를 통해 암호화되어 입·출력되므로 기존의 자기띠 방식의 카드보다 안전성 면에서 탁월하며, 기억용량이 크기 때문에 의료보험증, 주민등록증, 운전면허증 등 종합카드로서의 기능도 겸할 수 있다는 장점이 있다. 그러나 이를 널리 보급시키기 위해서는 IC카드 및 IC카드 판독기를 다량으로 공급하는데 막대한 초기투자비용이 필요하기 때문에 투자비용을 누가 부담하는가(상점, 소비자, 발행기관)가 보급의 관건이 된다.

그러나 네트워크형은 컴퓨터 하드디스크에 소프트웨어만 설치하면 되기 때문에 보급에 따른 막대한 신규투자를 필요로 하지 않는다. 다만 결제정보가 오픈 네트워크를 통해 전달되기 때문에 기존의 PC통신망을 이용하는 것보다는 더욱 정교한 보안기술을 필요로 하고 있다.[10]

한편 전자화폐는 기존의 결제 수단을 전자 신호를 통해 대체하는 방법에 따라 분류할 수도 있다(제일금융연구원, 1997). 먼저 선불카드에 재충전 기능을 추가시킨 선불카드형 전자화폐를 들 수 있다. 이것은 IC칩이 내장되어 있어서 ATM을 통해 카드의 잔고를 늘리거나 재충전할 수 있으며 위조가 어렵다는 점에서는 자기띠 방식의 기존의 선불카드보다 상대적으로 유용성이 크다. 그러나 개인 간 자금이체나 전자상거래 상의 전자결제가 어려워 화폐로서의 경제성은 그다지 크지 않다고 하겠다.

둘째로, 기존의 신용카드를 인터넷에서 사용할 수 있도록 한 신용카드형 전자화폐가 있다. 이것은 컴퓨터를 통해 자신의 신용카드 정보를 제공하는 방법으로 전자상거래의 결제수단으로 활용하는 것인데 CyberCash나 First Virtual 등이 현재 사용 중에 있는 대표적인 신용카드형

10) IC카드형과 네트워크형은 현재로서는 휴대성 측면에서 엄밀히 구분되지만 조만간 기술의 진전으로 양자의 겸용이 보편화될 것으로 예상되기 때문에 장기적으로는 이러한 구분이 무의미해질 가능성이 높다.

전자화폐들이다.

셋째로, 자신의 컴퓨터 상에서 전자수표를 발행해 각종 결제수단으로 사용하는 수표형 전자화폐를 들 수 있다. Netbill이나 NetCheque로 대표되는 전자수표는 기존의 수표와는 달리 인터넷을 통해 자신의 컴퓨터에서 발행한 당좌수표를 결제 상대방에게 송신하는 것이다. 수표형 전자화폐의 경우 현금가치를 은행에 저장시키고 거래당사자 간에는 은행계좌 간 자금이동을 위한 전자증서(전자수표)만 유통되기 때문에 안전하게 자금을 보관할 수 있을 뿐만 아니라 거액의 자금결제에도 용이한 결제수단이 된다.

넷째로, 현금 자체를 전자신호로 변환시킨 이후 유통시키는 현금형 전자화폐가 있다. 여기에는 IC카드형 전자화폐인 E-cash나 네크워크형 전자화폐의 대명사인 Mondex를 대표적인 예로 들 수 있는데, 특성 상 현재 사용하고 있는 현금과 성격이 매우 유사하기 때문에 다른 전자화폐보다 익명성에 있어서 월등히 우수하다.

3.1.2. 기술적 분류에 의한 유형

전자화폐의 기술적 분류에 의한 유형으로서는, (a) 전자화폐의 가치 형태, (b) 유통형태(양도성의 유무), (c) 가치정보의 관리장소, (d) 센터의 접속 유무, (e) 사용하는 암호기술 등이 있다. 여기서는 (a)~(d)의 항목의 조합을 근거로 모델을 나타내고, 각각에 대해서 (e)의 항목인 사용하는 암호기술의 선택 방법에 의해 전자화폐의 도입 타당성을 위한 분석 모델을 만들 수 있다(中山 靑司・松本 勉・太田和夫, 1999). 그러면 전자화폐의 모델화 작업을 위해 우선 네 가지 기술적 요인에 의한 유형을 분류해 보기로 한다.

먼저 가치형태의 특성 상 전자화폐를 잔고관리형과 전자증서형으로 분류할 수 있다. 잔고관리형은 전자지갑 등에 충전되어 있는 잔고금액을 상시 관리하는 방법으로서 거래 때마다 이 잔고정보의 갱신에 의해 결제처리를 한다. 한편 전자증서형은 데이터 자체가 가치를 가진다는 개념에서 만들어지기 때문에 액면전액, 식별번호 등의 정보를 가지고, 전자증서 형태로 교환됨으로써 결제처리를 한다.

둘째로 유통형태(양도성 유무) 즉 센터를 거치지 않고 한 이용자가 다른 이용자에게 전자화폐의 양도가 가능한가 어떤가에 따라 쌍방향 개방형(open loop) 전자화폐와 일방향 폐쇄형(closed loop) 전자화폐로 분류할 수 있다. Mondex와 같이 제3자에게 양도 가능한 전자화폐를 쌍방향 개방형 전자화폐[11]라고 한다. 그러나 현재 도입되고 있는 전자화폐 중에서 개인 간 자금이체가 가능한 것은 극히 일부분에 지나지 않는다. 이와 같이 개인 간 자금이체가 불가능한 전자화폐를 일방향 폐쇄형 전자화폐[12]라고 한다. 이것은 쌍방향 개방형 전자화폐보다 기술개발이 용이하며 법률적인 충돌이 적기 때문에 많은 나라에서 이 유형의 전자화폐를 실험・개발 중에 있다.

셋째로 가치정보의 관리장소를 기준으로 로칼관리형과 센터관리형으로 전자화폐를 분류할 수 있다. 즉. 로칼관리형은 전자지갑 내(로칼)에서 가치를 관리하는 전자화폐이고 센터관리형은 전자화폐의 발행기관(센터)에서 가치를 관리하는 전자화폐이다.

넷째로 센터 접속의 유무 즉 거래를 오프 라

11) 쌍방향 개방형에서는 일반 이용자와 상점 간에 기능적인 차이는 거의 없고, 상점도 이용자와 같다. 전자화폐가 이용자 간에 반복적으로 유통되어, 한동안 발행기관에 환류되지 않을 수도 있다.

12) 일방향 폐쇄형에서는 전자화폐의 흐름이 일방향적이며, 이용자와 상점은 기능적으로 서로 다르다.

인에 의해 가능한지 혹은 반드시 온라인으로 센터에 문의해서 처리해야 하는지에 따라 오프라인형과 온라인형으로 분류할 수 있다.

3.1.3. 전자화폐의 모델 유형

이상에서 살펴본 바와 같이 일반적 분류에 의한 유형 중 IC카드형과 네트워크형은 최근 겸용화 추세에 있어 본 연구의 분석방법에는 적합하지 않다고 판단되어 여기서는 기술적 분류에 의한 모델 유형에 따라 전자화폐의 유형을 분석하기로 하였다.[13] 그러나 센터에서 가치를 관리하기 위해서는 센터 접속이 필수조건이 된다든가, 전자증서형에서는 가치관리장소가 로칼로 한정되어 있는 등, 현실적으로는 모순적이거나 무의미한 조합도 있기 때문에 모든 조합이 전자화폐가 되는 것은 아니다. <표 1>, <표 2>는 각 조합에 있어서 전자화폐의 성립 가능성을 나타낸 것이며, 실제로는 잔고관리형의 경우 네 가지 모델과 전자증서형의 경우 세 가지 모델을 분석모델로 정하고 각각에 대한 안전성을 평가한다.[14]

3.2. 전자화폐의 모델 유형별 암호기술의 선택

각 전자화폐 모델에서 이용되는 암호기술로서 크게 나누면 공통키 암호를 이용한 것, 공개키 암호(내지 디지털 서명방식)를 이용한 것, 그 중간적인 것 등 세 종류를 생각할 수 있다. 본 연

〈표 1〉 잔고관리형 전자화폐의 모델 유형

유통형태 (양도성 유무)	일방향 폐쇄형				쌍방향 개방형			
가치관리장소	로 칼		센 터		로 칼		센 터	
센 터 접 속	오프라인	온라인	오프라인	온라인	오프라인	온라인	오프라인	온라인
모 델 유 무	유 (모델 I)	유 (모델 I')	무 (☆1)	유 (모델 II)	유 (모델 III)	무 (☆2)	무 (☆1)	무 (☆2)

〈표 2〉 전자증서형 전자화폐의 모델 유형

유통형태 (양도성 유무)	일방향 폐쇄형				쌍방향 개방형			
가치관리장소	로 칼		센 터		로 칼		센 터	
센 터 접 속	오프 라인 (사후검증)	온 라 인 (즉시검증)	오프라인	온 라 인	오프 라인 (사후검증)	온 라 인 (즉시검증)	오프라인	온 라 인
모 델 유 무	유 (모델 IV)	유 (모델 V)	무 (☆3)	무 (☆3)	유 (모델 VI)	무 (☆2)	무 (☆3)	무 (☆3)

☆1 : 센터에 온라인 접속시키지 않고 센터에서 잔고를 관리하는 것은 불가능하다.
☆2 : 쌍방향 개방형은 한 이용자에서 다른 이용자에게로 센터를 개재시키지 않고 가치를 이전시키는 것이 가능하며, 이러한 의미에서 매번 거래 때마다 센터에 접속하여 정보를 주고받는 경우는 쌍방향 개방형이라고 말할 수 없다.
☆3 : 전자증서형은 데이터 자체가 가치를 가진다는 개념에서 만들어지는 방법이기 때문에 가치관리장소는 로칼 밖에 없다.

13) 이 분석 모델은 中山 青司·松本 勉·太田和夫(1999)의 분류모델을 참조하여 우리 나라의 경우 어떤 유형의 전자화폐를 도입하는 것이 안전성과 효율성 측면에서 우월한가를 분석하는 데 적용하여 보았다.

14) 현재 각국에서 실증실험·실용화가 추진되고 있는 전자화폐 중에는 보안 방법을 명확히 하지 않는 경우도 많은데, 그것도 역시 위의 모델로 유형화시킬 수 있을 것이다.

구에서는 앞에서 검토한 실현가능한 전자화폐의 모델 유형에 대해서, 이들의 암호기술을 이용한 안전성을 분석하기로 한다. 그리고 잔고관리형과 전자증서형에서는 실현방식의 차이로 암호기술의 이용 방법이 다르기 때문에 선택 묶음의 내용은 아래와 같이 각각 다르다.

3.2.1. 잔고관리형 전자화폐

(1) 공통키형의 경우

공통키형은 본인 확인 및 데이터 송·수신에 공통키 암호를 사용하는 방식이며, 발행기관(센터)에서는 공통비밀키(K)를 보유하고 있다.

수취자는 점포명·요구금액·현재시각 등 DT라는 송신내역을 지불자에게 송신하고, 지불자는 공통비밀키 K를 사용하여 식별자 I_A, 점포명·요구금액·현재시각 등 DT를 암호화함으로써 지불정보 $E_K(I_A, DT)$를 작성하여 수취자에게 송신함과 동시에 보유잔고를 감액시킨다. 이 때 수취자는 넘겨받은 지불정보를 공통비밀키 K를 사용하여 복호화하고, 미리 송부한 DT가 포함되어 있는지를 확인한 후 보유잔고를 증액시킨다.

(2) 靜的 認證을 요하는 공통키형의 경우

정적 인증을 요하는 공통키형은 데이터 송·수신에 공통키 암호를 사용하는데, 본인 확인은 센터의 비밀키에 의해 디지털 서명된 증명서 제시에 의해 이루어지는 방법이다. 이 때 발행기관(센터)에서는 공통비밀키(K)와 센터의 비밀키(S_{KC}) 및 공개키(P_{KC})를 보유하고 있다.

수취자는 점포명·요구금액·현재시각 등 DT라는 송신내역을 지불자에게 송신하고, 지불자는 공통비밀키 K를 사용하여 센터의 증명서 $S_C(I_A)$, 점포명·요구금액·현재시각 등 DT를 암호화함으로써 지불정보 $E_K(S_C(I_A), DT)$를 작성하여 수취자에게 송신함과 동시에 보유잔고를 감액시킨다. 이 때 수취자는 넘겨받은 지불정보를 공통비밀키 K를 사용하여 복호화하고, 센터의 증명서를 센터의 공개키 P_{KC}를 사용하여 검증함과 동시에 미리 송부한 DT가 포함되어 있는지를 확인한 후 보유잔고를 증액시킨다.

(3) 動的 認證을 요하는 공개키형의 경우

동적 인증을 요하는 공개키형은 본인 확인을 공개키 암호를 이용한 동적 인증(지불 시에 송신내역<점포명·금액·시각 등>에 대한 디지털 서명을 생성)에 의해 행하는 방식인데, 나아가 데이터 송·수신에 암호를 사용하는 경우도 있다. 이 경우 발행기관(센터)에서는 센터의 비밀키(S_{KC}) 및 공개키(P_{KC})를 보유하고 있다.

수취자는 점포명·요구금액·현재시각 등 DT라는 송신내역을 지불자에게 송신하고, 지불자는 비밀키 S_{KA}를 사용하여 DT를 서명함으로써 지불정보 $S_A(DT)$를 작성하여 공개키증명서 $S_C(P_{KA})$와 함께 수취자에게 송신함과 동시에 보유잔고를 감액시킨다. 이 때 수취자는 넘겨받은 지불정보를 센터의 공개키 P_{KC}를 사용하여 공개키증명서로부터 얻어낸 지불자의 검증키 P_{KA}에 의해 검증한 후 보유잔고를 증액시킨다.

3.2.2. 전자증서형 전자화폐

(1) 공개키형의 경우

공개키형은 본인확인 및 데이터 송·수신에 공통키 암호를 사용하고, 발행기관이 할당한 식별번호 등을 포함하는 전자증서(디지털 서명없이)를 송신함에 따라 가치를 이전하는 방법이며, 발행기관(센터)에서는 공통비밀키(K)를 보유하고 있다.

수취자는 점포명·요구금액·현재시각 등 DT

라는 송신내역을 지불자에게 송신하고, 지불자는 공통비밀키 K를 이용하여 지불에 사용되는(요구금액이 액면금액 V와 일치하는) 전자증서 식별번호 N_O, 이용자의 식별자 I_A, 요구금액 및 현재시각 등 DT를 서명함으로써 지불정보 $E_K(I_A, N_O, DT)$를 작성하여 수취자에게 송신한다. 이 때 수취자는 넘겨받은 지불정보를 공통비밀키 K를 사용하여 검증한다.

(2) 정적 인증을 요하는 공개키형의 경우

정적 인증을 요하는 공개키형은 본인 확인을 센터의 비밀키에 의해 디지털 서명된 증명서 제시에 의해 이루어지는 방법인데, 전자증서 자체도 센터의 비밀키에 의해 디지털 서명된다(블라인드 서명을 사용하는 것을 가정). 이 때 발행기관(센터)에서는 센터의 비밀키(S_{KC}) 및 공개키(P_{KC})를 보유하고 있다.

수취자는 점포명·요구금액·현재시각 등 DT라는 송신내역을 지불자에게 송신하고, 지불자는 지불에 사용되는(요구금액이 액면금액 V와 일치하는) 전자증서 $S_C(S_C(I_A), N_O, V)$를 선택하여 센터의 증명서 $S_C(I_A)$와 함께 수취자에게 송신한다. 이 때 수취자는 넘겨받은 전자증서 및 센터의 증명서를 센터의 공개키 P_{KC}를 사용하여 검증한다.

(3) 동적 인증을 요하는 공개키형의 경우

동적 인증을 요하는 공개키형은 본인 확인을 공개키 암호를 이용한 동적 인증(지불 시에 송신내역<점포명·금액·시각 등>에 대한 디지털 서명을 생성)에 의해 본인 확인을 하는 방법인데, 전자증서 자체는 센터의 비밀키에 의해 디지털 서명된다(블라인드 서명을 사용하는 것을 가정). 발행기관(센터)에서는 센터의 비밀키(SKC) 및 공개키(PKC)를 보유하고 있다.

수취자는 점포명·요구금액·현재시각 등 DT 및 수취자의 공개키증명서 $S_C(P_{KB})$를 송신내역으로서 지불자에게 송신하고, 지불자는 지불에 사용되는(요구금액이 액면금액 V와 일치하는) 전자증서 $S_C(S_C(P_{KA}), N_O, V)$를 선택하여 수취자의 공개키증명서 $S_C(P_{KB})$, 점포명·요구금액·현재시각 등 DT에 서명한 양도증 $S_A(S_C(P_{KB}), DT)$와 함께 수취자에게 송신한다. 이 때 수취자는 넘겨받은 전자증서 및 양도증을 센터의 공개키 P_{KC}를 사용하여 검증한다.

Ⅳ. 전자화폐의 모델 유형별 도입 타당성 분석

4.1. 분석 대상과 방법

본 장에서는, 기술적인 요인에 의한 전자화폐의 모델 유형 방식이 기존의 전자화폐의 유형을 포괄하고 있을 뿐만 아니라 새로운 전자화폐의 개발 유형에도 적합한 분류방식이라고 판단되어 이 유형의 전자화폐에 대한 도입 타당성 분석을 그 대상으로 삼았으며, 현재 개발된 여러 가지 암호기술과 어떤 방식으로 결합이 되었을 때 가장 안전하고 효율적인 전자화폐가 될 수 있을 것인지를 중점적으로 분석하고 도입에 따른 타당성이 다소 떨어지거나 불안전한 모델의 경우 향후 부정변조에 대한 내성 장치를 개발, 기술적으로 보완함으로써 갑작스러운 도입에 따른 경제적인 충격을 최소화하고 중·장기적으로 가장 효율적인 전자화폐를 개발·도입하는데 필요한 기초연구자료를 제시하고자 한다.

전자화폐는 암호기술이나 부정변조에 대한 내성 기술 등의 다양한 요소기술을 합쳐 구성함으로써, 도입에 따른 위험을 줄일 수 있다. 그러나 이들의 요소기술은 절대적인 안전성을 가지고 있다고 단정할 수는 없다. 따라서 개개의 요소기술 중, IC카드의 부정변조에 대한 내성에 의존하지 않고 전자화폐를 구성한 경우, 그 논리적인 구성방법의 차이로, 전자화폐의 도입에 따른 타당성 분석에 어떤 차이가 생기는지를 살펴본다.

이같은 분석 결과를 토대로 역으로 부정변조에 대한 내성 장치가 어떤 경우에 필요한가, 또한 그 부정변조에 대한 내성 장치에 요구되는 안전성의 강도는 어떤 정도인가 등을 검토하기로 한다. 그리고 여기서 분석 대상으로 하는 것은, 특히 「가치를 부정하게 입수한 행위」에 대한 안전성이며, 결제를 방해하거나 전자화폐 시스템 자체를 파괴하려 하는 행위 등에 대한 안전성은 대상으로 하지 않는다. 또한 「가치를 부정하게 입수한 행위」라고 하더라도, 전자화폐가 들어간 IC 카드 자체를 훔쳐 사용하는 류의 부정행위에 대해서는 통상 돈과 같이 물리적인 도난에 대한 안전대책의 문제이며, 전자화폐의 고유의 사정은 아니므로, 직접 검토 대상에서 제외하였다.

평가는 구체적으로는 전자화폐를 몇 개의 모델 유형으로 나누어, 예컨대 이용자 자신이 가지고 있는 정보를 사용해 어떠한 부정을 할 수 있는가(방지), 그것은 시스템을 관리함에 따라 검지할 수 있는 것인가(검지), 부정을 검지했을 때에 피해를 수습하기 위한 대책은 있는가(대응)라는 관점에서 발생할 수 있는 위험의 종류·정도·범위를 분석한다.

전자화폐를 몇 개의 모델로 분류하고 그 안전성을 평가하는데 있어서는 반드시 구체적인 전자화폐 프로젝트나 논문은 상정하지 않고 일반적인 전자화폐 모든 것에 대해서 적용가능한 결론을 도출하는 것을 목적으로 한다. 이를 위해 전자화폐의 보안에 영향을 주는 주요한 기술적 특징이나 기능에 대해서 선택 대안의 모든 조합을 후보로 들고, 그 중에서 현실적으로 얻을 수 있는 것을 분석의 대상 모델로 선택한다.

4.2. 전제조건과 분석 항목

전자화폐의 도입 타당성을 분석하는 데 있어서는, 불특정 다수의 이용자가 불특정 다수의 상점에서 전자화폐를 사용해서 지불하는 상황을 상정한다. 그리고, 각 이용자, 상점이 스스로 보유하는 IC카드(부정변조에 대한 내성 장치가 없는 경우)나 컴퓨터 기억장치 속에 있는 전자화폐에 관한 정보를 읽어내서 이를 이용함에 따라 어떤 부정행위를 할 수 있을 것인가를 분석한다. 또한 발행기관(등록기관 포함)의 보안 대책이 불충분하며, 내부자에 의한 범행이 가능하다는 가정 하에 보유하고 있는 비밀키 등의 정보가 외부로 유출된 경우, 그것에 의해 어떤 부정이 생길 것인가에 대해서도 분석한다.

도입 타당성의 분석은 본장에서 정리한 실현가능한 모델에 대해, 각각 세 종류의 암호기술을 적용한 전자화폐 실현방식을 상정하고, 생각할 수 있는 부정의 종류(위조, 변조, 복제, 착취 등), 부정검지의 여부(부정 발생 사실, 부정 발생 특정장소), 검지된 경우 부정행위를 억제하기 위한 대응책의 유무를 분석한다. 특히 이용자가 지불정보를 위조할 경우에 대해서는, 다른 이용자인 것처럼 행세(위장)함으로써 부정이 가능한가라는 관점에서도 안전성 수준을 구별하여 분

석하고, 상점이 환류정보를 위조할 수 없다고 판단된 경우에 대해서도 다른 이용자와의 결탁을 통해 부정이 가능한가에 대해서 분석한다(中山 靑司·松本 勉·太田和夫, 1999). 아울러 사용하는 공통키 암호, 공개키 암호, 디지털 서명 방식은 적절한 알고리즘이 이용되고 있을 뿐만 아니라, 충분한 키의 길이를 설정하고 있기 때문에 안전하며, 해독이나 서명의 위조는 없는 것으로 가정한다. 도입 타당성 분석을 위한 항목 및 그 내용은 다음과 같다.

첫째, 지불정보의 위조(이용자가 보유하는 정보를 이용한 부정행위)이다.

이것은 이용자가 스스로 보유하는 비밀정보를 이용함으로써 지불정보를 위조하여 상점에 넘기는 부정행위를 의미한다. 특히 (a) 위조된 지불정보가 본래 이용자 본인의 것인가(본인), (b) 어떤 특정 이용자로서의 지불정보를 위조한 것인가(특정인), (c) 임의의 이용자로서의 지불정보를 위조한 것인가(불특정인)에 의해서 부정행위의 추적이 가능한가 어떤가의 차이가 발생하기 때문에, 이를 특히 구별하여 분석할 필요가 있다.

둘째로 환류정보의 위조(상점이 보유하는 정보를 이용한 부정행위)이다.

이 경우에는 (a) 결탁이 없는 경우의 위조와 (b) 결탁이 있는 경우의 위조로 나누어 분석할 수 있다. 전자의 경우는 상점이 이용자로부터 받은 매상(수취정보)을 위조하여 은행에 환류시킴으로써 가치를 입수하는 부정행위인데, 상점과 은행 간의 거래는 익명성이 없는 상태에서 행해지므로 상점은 역시 도주하는 형태의 부정을 행하는 것은 불가능하다. 한편 후자의 경우는 상점이 특정의 이용자와 결탁하고, 이용자가 보유하는 비밀정보도 이용함으로써 비로소 실행 가능케 되는 부정행위를 말한다.

셋째로, 발행기관(등록기관 포함) 정보에 의한 위조(발행기관의 정보를 이용한 부정행위)이다.

부정행위자가 발행기관(등록기관 포함)이 보유하는 비밀정보를 부정하게 입수한 뒤, 이것을 이용하여 발행정보 내지 지불정보를 위조함으로써 가치를 입수하는 부정행위이다. 발행기관에 의한 비밀키 등의 정보관리가 취약하거나, 내부자에 의한 부정행위가 가능한 경우에 상정되는 위조이다.

4.3. 분석 결과

각 전자화폐 모델에 있어서 (a) 지불정보의 위조, (b) 환류정보의 위조, (c) 발행기관 정보에 의한 위조에 대해서 각각 분석하였다.

아래의 내용은 잔고관리형 세 종류(<모델Ⅰ>~<모델Ⅲ>), 전자증서형 세 종류(<모델Ⅳ>~<모델Ⅵ>)에 대해서 분석한 결과이다.[15][16]

15) 〈모델Ⅰ'〉(잔고관리형·일방향적 폐쇄형·로칼관리·온라인형)에 대해서는, 본고의 검토 범위에서 안전성을 분석하는 관점에서는 센터 접속의 필연성이 인정되지 않을 뿐만 아니라, 〈모델Ⅰ〉과 같은 결과가 나왔기 때문에 여기서는 분석을 하지 않았다.

16) 분석 결과에서 사용되고 있는 기호의 의미는 아래와 같다.

A : 공격대상의 전자지갑의 이용자	
A′: 다른 특정 이용자	
A^* : 임의의 이용자	
K : 비밀키	
$E_K(X)$: 데이터 X를 K로 암호화	
I_A : 이용자 A의 익명의 식별자	
P_{KA}, S_{KA} : 이용자 A의 공개키, 비밀키	
P_{KB}, S_{KB} : 이용자 A의 공개키, 비밀키	
P_{KC}, S_{KC} : 센터 C의 공개키, 비밀키	
Sc(X) : 센터 C에 의한 데이터 X에의 서명	
DT : 점포명, 금액, 시각 등	
DT′ : 임의로 지정한 점포명, 금액, 시각 등	
N_O : 전자증서의 식별번호	
V : 전자증서의 액면금액	
V′ : 임의로 지정한 전자증서의 액면금액	

각 전자화폐의 모델 유형별로 지불정보의 위조, 환류정보의 위조 및 발행기관의 정보를 이용한 위조에 의한 피해 상황을 각각 정리한 것을 <표 4>~<표 6>에 나타냈다.[17] 그리고 각 표에서 도입 타당성 분석항목으로서 공격 성공 가능성 여부, 공격 성공시 검지 가부, 검지 가능시 대응책 유무 등에 대한 평가등급을 안전성이 가장 높은 A등급에서 가장 낮은 D등급까지 네 단계로 구분하여 분석하였다.

한편 지불정보의 위조 등의 가치를 부정하게 입수하는 공격이 불가능한 유형의 전자화폐는, 그 자체로서 안전성을 확보하고 있기 때문에, IC카드 등에 부정변조에 대한 내성 장치를 할 필요가 없다(안전성 레벨A). 그리고 가치를 부정하게 입수하는 공격이 성공할 가능성이 있다고 하더라도, 사후적으로 부정행위자의 신원을 확인할 수 있는 등, 이를 검지하여 방지하는 효과적인 대응책이 존재하는 유형의 전자화폐(안전성 수준B)는, 도주할 수 없는 등의 한정된 운용 환경 하에서는 어느 정도는 안전하다고 하지만 부정변조에 대한 내성 장치(기기)를 갖춤에 따라, 더욱 안전성을 높일 수 있다. 한편 이용자가 스스로 보유한 비밀정보를 기초로, 지불정보를 위조함으로써 가치를 부정하게 입수하는 공격이 성공하고, 그 사실을 검지할 수 없는 유형의 전자화폐(안전성 수준D)나, 검지는 가능하더라도, 위조 등에 의한 피해를 방지하는 대응책을 전혀 강구할 수 없는 유형의 전자화폐(안전성 수준C)는, 이것만으로는 필요한 안전성을 확보할 수 없으며, IC카드 등의 부정변조에 대한 내성 장치를 이용함으로써 이용자가 스스로 보유한 비밀정보에 부정하게 접근할 수 없도록 할 필요가 있다. 전자화폐를 설계할 때에는, 일정 비용 제약 하에서, 필요한 機器나 편리성을 실현하면서, 이러한 안전성 수준을 현저하게 높이는 것이 필요하다. 각 전자화폐 모델 유형에 있어서 각종 위조에 관한 분석 결과를 토대로 부정변조에 대한 내성 장치의 필요성에 대해 정리한 것이 <표 3>이다.

4.3.1. 잔고관리형 전자화폐의 도입 타당성 분석결과

(1) 지불정보 위조의 경우

잔고관리형에서는 로칼방식으로 가치를 관리하는 오프라인형의 전자화폐는 기본적으로는 가치의 부정한 창출이 자유롭게 이루어질 수 있기 때문에 미리 부정변조에 대한 내성 장치를 갖춘 IC카드 등의 부가적인 안전대책을 강구할 필요가 있다. 센터에서 가치를 관리하는 온라인형의

〈표 3〉 전자화폐의 안전성 수준과 부정변조에 대한 내성 장치의 필요성

안전성 수준	위조에 대한 사전방지 가능성	위조에 대한 검지 가능성	위조에 대한 사후 대응 가능성	안전성 판단	부정변조에 대한 내성 장치의 필요성
수준 A	공격 불가(A)	-	-	안 전	불 필 요 함
수준 B	공격 성립(D)	검지 가능(A)	대응 가능(A)	다소 안전	바 람 직 함
수준 C	공격 성립(D)	검지 가능(A)	대응 불가(D)	위 험	필 수 적 임
수준 D	공격 성립(D)	검지 불가(D)	-	위 험	필 수 적 임

17) 〈표 4〉~〈표 6〉에서의 □는 부정변조에 대한 내성 장치가 필수적인 경우이고, ▨는 부정변조에 대한 내성 장치가 바람직한 경우이며, ▩는 부정변조에 대한 내성 장치가 불필요한 경우를 나타낸다.

전자화폐에서는, 가치가 부정하게 창출될 위험은 없지만, 본인 인증의 안전성이 확보되지 않는 경우에는 다른 이용자의 가치가 도난당할 위험이 있다. 특히 암호방식으로서 공통키 암호나 공개키 암호에 의한 정적 인증을 사용하는 유형의 전자화폐는, 도청으로 본인 인증을 위한 정보 등이 도난당하면 그렇게 될 가능성이 크기 때문에 공격받을 위험성이 있다. 따라서 잔고관리형의 전자화폐에서 부정변조에 대한 내성 장치에 의존하지 않고도 안전한 것은 센터에서 가치를 관리하는 일방향적 폐쇄형의 전자화폐에서 암호기술로서 공개키 암호를 이용한 동적 인증을 사용하는 유형이 된다.

(2) 환류정보 위조의 경우

한편, 잔고관리형의 전자화폐는, 센터에서 잔고를 관리하고 있지 않는 경우(로칼만으로 잔고를 관리하고 있는 경우)는, 가치를 부정하게 창출하는 유형의 공격이 가능하다(부정변조에 대한 내성장치가 필요). 무엇보다도, 이 경우 가치를 넘겨 받았을 때 로그(거래 이력)도 발행기관에 전송하도록 한다면 안전하지만, 그렇더라도 상점이 다른 이용자와 결탁한 경우에는 공격을 받을 수 있다는 것을 알 수 있다. 또한 센터에서 잔고를 관리하는 경우, 상점이 일시적으로 다른 이용자의 가치를 빼돌리는 것은 가능하지만, 빼돌려진 이용자의 신고로 부정 사실이 발각될 뿐만 아니라, 센터의 로그를 확인함으로써 도난당한 가치가 어느 상점의 전자화폐 출납구좌에 입금되었는가를 파악할 수 있기 때문에, 부정이 행해진 전자화폐 출납구좌를 동결하거나, 구좌 주인을 잡을 수 있어 피해는 한정된다(부정변조에 대한 내성이 있으면 더욱 안전성이 향상). 또한 가치를 주고 받을 때 로그도 발행기관에 전송하도록 한다면, 결탁이 없는 경우 이용자로부터 받은 전자화폐의 환류정보를 위조할 수 없으므로 더욱 안전하다(부정변조에 대한 내성 장치는 불필요).

(3) 발행기관의 정보를 이용한 위조의 경우

발행기관의 정보를 이용한 위조라는 관점에서 보면, 잔고관리형의 전자화폐의 경우, 센터에 온라인으로 접속해서 거래처리가 행해지는 모델 유형(<모델 Ⅱ>)에서는 다른 이용자의 잔고를 빼돌리는 종류의 위조 밖에 있을 수 없고(공개키 암호를 이용한 동적 인증으로 본인 확인을 한다면 이것도 방지), 게다가 사후적으로 부정을 행한 전자지갑을 확인할 수 있으므로, 상대적으로 안전성은 높다.

4.3.2. 전자증서형 전자화폐의 도입 타당성 분석결과

(1) 지불정보 위조의 경우

전자증서형의 전자화폐에서는 암호기술로서 공개키 암호를 사용한 유형이라면, 기본적으로 위조를 할 수 없다. 여기서 문제가 되는 것은, 이용자 본인이 보유하는 전자화폐의 이중사용이나, 도청 등에 의해 입수한 다른 이용자가 보유하는 전자화폐의 부정사용이지만, 이들에 대해서는 온라인으로 즉시 검증이 가능하기 때문에 이를 막을 수 있다. 또한, 온라인으로 즉시검증을 행하지 않더라도, 암호방식으로서 공개키 암호의 동적 인증을 사용하는 유형이라면, 도청 등에 의해 입수한 다른 이용자의 전자화폐가 부정사용되는 것을 막을 수 있다. 이 경우에도, 이용자 본인이 보유하는 전자화폐를 이중사용하는 것은 가능하지만, 암호기술에 의해 부정행위자를 사후적으로 신분을 확인할 수 있기 때문에, 도주할

수 없는 그러한 운용 환경 하에서는 안전하다고 할 수 있다. 부정변조에 대한 내성기기 등의 부가적인 안전대책을 갖추면 더욱 더 안전하다고 할 수 있겠다.

(2) 환류정보 위조의 경우

환류정보의 위조라는 관점에서 보면, 전자증서형의 전자화폐는, 환류 시에는 어느 모델 유형이라도 결과적으로 온라인으로 체크가 되므로 안전하다. 따라서 부정변조에 대한 내성 장치는 필요 없다..

(3) 발행기관의 정보를 이용한 위조의 경우

발행기관의 정보를 이용한 위조라는 관점에서 보면, 잔고관리형의 전자화폐의 경우, 센터에 온라인으로 접속해서 거래처리가 행해지는 모델 유형(모델Ⅱ)에서는 다른 이용자의 잔고를 빼돌리는 종류의 위조 밖에 있을 수 없고(공개키 암호를 이용한 동적 인증으로 본인 확인을 한다면 이것도 방지), 게다가 사후적으로 부정을 행한 전자지갑을 확인할 수 있으므로, 상대적으로 안전성은 높다.

한편 전자증서형의 경우는 발행기관의 정보를 이용함으로써 임의의 전자증서, 양도증을 작성하는 것이 가능하다. 단, 환류 시의 발행기관에 의한 이중사용 체크 방법에 의해 이를 발견함으로써 부당 사용을 방지할 수 있다. 전자화폐의 발행에 블라인드 서명을 사용함으로써 익명성을 실현하고 있는 유형의 전자화폐에서는, 발행 시에 전자증서 식별번호를 등록할 수 없기 때문에, 통상 환류 시에 등록을 하고, 만약 이미 등록이 되어 있으면 이것은 이중사용된 전자화폐로 간주한다. 따라서 발행기관의 비밀키를 사용해서 새롭게 위조된 전자증서는 원본과 구별되지 않고 수용·처리되어 버린다. 이에 반해 전자화폐 발행 시에 전자증서 식별번호를 등록할 수 있는 전자화폐에서는 환류 시에 삭제·처리를 하고, 만약 삭제해야 할 식별번호가 존재하지 않으면 부정한 전자화폐로 판단되기 때문에, 정당한 발행기관의 비밀키를 사용한 전자증서라고 하더라도 이것은 위조라고 판단되어 안전성이 높다.

〈표 4〉 지불정보 위조에 대한 분석결과표

			잔고관리형 전자화폐			전자증서형 전자화폐		
암호기술	이용정보 대 상	분석 항목	〈모델 I〉	〈모델 II〉	〈모델 III〉	〈모델 IV〉	〈모델 V〉	〈모델 VI〉
공통키형	본 인	공격 성공 가능성 여부	D_1	A_1	D_1	D_1	A_1	D_1
		공격 성공시 검지 가부	D_2	-	D_2	A_2 ☆6	-	A_2 ☆6
		검지 가능시 대응책 유무	-	-	-	C_3 ☆7	-	C_3 ☆7
	특 정 인	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1	D_1	C_1 ☆9	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	A_2 ☆6	A_2 ☆6	A_2 ☆6
		검지 가능시 대응책 유무	-	C_3 ☆3	-	C_3 ☆7	D_3	C_3 ☆7
	불특정인	공격 성공 가능성 여부	D_1	C_1 ☆4	D_1	D_1	A_1	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	A_2 ☆6	-	A_2 ☆6
		검지 가능시 대응책 유무	-	C_3 ☆3	-	D_3	-	D_3
정적 인증을 요하는 공통키형	본 인	공격 성공 가능성 여부	D_1	A_1	D_1	C_1	A_1	C_1
		공격 성공시 검지 가부	D_2	-	D_2	A_2 ☆6	-	A_2 ☆6
		검지 가능시 대응책 유무	-	-	-	A_3 ☆8	-	A_3 ☆8
	특 정 인	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1 ☆5	C_1	A_1☆10	C_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	A_2 ☆6	-	A_2 ☆6
		검지 가능시 대응책 유무	-	C_3 ☆3	-	D_3	-	D_3
	불특정인	공격 성공 가능성 여부	A_1	A_1	D_1 ☆5	A_1	A_1	A_1
		공격 성공시 검지 가부	-	-	D_2	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-
동적 인증을 요하는 공개키형	본 인	공격 성공 가능성 여부	D_1	A_1	D_1	C_1	A_1	C_1
		공격 성공시 검지 가부	D_2	-	D_2	A_2 ☆6	-	A_2 ☆6
		검지 가능시 대응책 유무	-	-	-	A_3 ☆8	-	A_3 ☆8
	특 정 인	공격 성공 가능성 여부	A_1	A_1	D_1 ☆5	A_1	A_1	A_1
		공격 성공시 검지 가부	-	-	D_2	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-
	불특정인	공격 성공 가능성 여부	A_1	A_1	D_1 ☆5	A_1	A_1	A_1
		공격 성공시 검지 가부	-	-	D_2	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-

A_1: 공격불가(매우 안전), B_1: 운용당시 공격방지(다소 안전), C_1: 부분공격 성립(다소 불안전), D_1: 공격성립(매우 불안전)

A_2: 검지가능(매우 안전), D_2: 검지불가(매우 불안전)

A_3: 대응가능(매우 안전), B_3: 상당정도 대응가능(다소 안전), C_3 : 어느 정도 대응 가능(다소 불안), D_3: 대응불가(매우 불안전) - : 분석불요

☆1 : 도청에 의해 I_A를 입수가능한 A'의 잔고를 탈취할 수 있음.

☆2 : 도난당한 A'(A*)가 자신의 잔고가 감소된 것을 알아채고, 부정 사실을 확인할 수 있음. 또한 센터의 로그에 의해 A'(A*)로부터 어떻게 전자지갑에대해 자금이동이 있었는가를 파악할 수 있음.

☆3 : 부정행위가 이루어진 전자지갑을 거래정지함으로써 피해는 더 이상 발생 불가능함.

☆4 : 임의로 선택한 식별자 I_{A^*}가 실제로 존재하면 A*의 잔고를 탈취할 수 있음.

☆5 : 완전한 익명성이 보장되기 때문에 본인을 마치 제3자인 것처럼 위장하여 실질적으로 공격이 성립하는 경우

☆6 : 사후적인 센터 체크에 의해 검지가 가능하며, 부정행위자 및 피해자의 신원 확인이 가능함.

☆7 : 상점이 핫리스트를 입수할 수 있다면 체크가 가능함.

☆8 : 발견된 부정행위자의 신원을 확인할 수 있는 정보를 근거로 부정행위자를 추적함.

☆9 : 도청(특히 발행시)한 A'의 증서를 미리 사용할 수 있다면 공격이 가능함.

☆10 : 도청한 A'의 증서를 미리 사용 가능하다면 공격이 가능하다. 그러나 증서는 발행시에 암호화되어 있기 때문에 도청이 곤란하고, 도청가능한 것은 사용 시로 한정되기 때문에 공격이 성공할 가능성을 그다지 크지 않다.

〈표 5〉 환류정보 위조에 대한 분석결과표

			잔고관리형 전자화폐			전자증서형 전자화폐		
암 호 기 술	결탁여부	분 석 항 목	〈모델 I 〉	〈모델 II 〉	〈모델 III 〉	〈모델 IV 〉	〈모델 V 〉	〈모델 VI 〉
공 통 키 형	무	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1	B_1 ☆5	A_1 ☆3	B_1 ☆5
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	-	-	-
		검지 가능시 대응책 유무	-	A_3 ☆3	-	-	-	-
	유	공격 성공 가능성 여부	-	A_1	-	B_1 ☆5	A_1 ☆3	B_1 ☆5
		공격 성공시 검지 가부	-	-	-	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-
정적 인증을 요하는 공개키형	무	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1	B_1 ☆5	A_1 ☆3	B_1 ☆5
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	-	-	-
		검지 가능시 대응책 유무	-	A_3 ☆3	-	-	-	-
	유	공격 성공 가능성 여부	-	A_1	-	B_1 ☆5	A_1 ☆3	B_1 ☆5
		공격 성공시 검지 가부	-	-	-	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-
동적 인증을 요하는 공개키형	무	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1	B_1 ☆5	A_1 ☆3	B_1 ☆5
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	-	-	-
		검지 가능시 대응책 유무	-	A_3 ☆3	-	-	-	-
	유	공격 성공 가능성 여부	-	A_1 ☆4	-	B_1 ☆5	A_1 ☆3	B_1 ☆5
		공격 성공시 검지 가부	-	-	-	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-
동적 인증의 로그도 전송하는 경우	무	공격 성공 가능성 여부	A_1	A_1	A_1	증서형은 항상 동적 인증 로그도 전송한다.		
		공격 성공시 검지 가부	-	-	-			
		검지 가능시 대응책 유무	-	-	-			
	유	공격 성공 가능성 여부	D_1	A_1 ☆4	D_1			
		공격 성공시 검지 가부	D_2	-	D_2			
		검지 가능시 대응책 유무	-	-	-			

A_1: 공격불가(매우 안전), B_1: 운용당시 공격방지(다소 안전), C_1: 부분공격 성립(다소 불안전), D_1: 공격성립(매우 불안전)

A_2: 검지가능(매우 안전), D_2: 검지불가(매우 불안전)

A_3: 대응가능(매우 안전), B_3: 상당정도 대응가능(다소 안전), C_3 : 어느 정도 대응 가능(다소 불안), D_3: 대응불가(매우 불안전)

- : 분석불요

☆1 : 즉시 거래가 있고, 상점이 식별자 I_A의 정보를 입수, A의 잔고를 탈취할 수 있음.

☆2 : 사후적으로 A는 자신의 잔고가 감소되고 있다는 사실을 알아채고, 부정 사실을 확인할 수 있음. 또한 센터의 로그에 의해 A로부터 어떻게 전자지갑 출납구좌에 대해 부정한 자금이동이 있었는가를 파악할 수 있음.

☆3 : 부정행위자의 전자지갑 출납구좌를 봉쇄하고 거래를 정지시킴.

☆4 : 잔고는 센터에서 관리되고 있기 때문에 상점과 결탁자의 정보에서는 양자 간의 가치이전만 가능함(즉 가치를 위조하는 것은 불가능함).

☆5 : 환류 후, 센터 체크가 종료할 때까지 얼마 안되는 사이에 환류에 걸맞는 금액의 자금을 개방할 경우는 일시적으로 이중 사용에 의한 도주가 가능케 되는데, 실제로는 익명 거래에서는 환류가 존재하지 않기 때문에, 부정이 알려질 것을 두려워하는 억제효과가 나타나는 것 이외에, 센터 체크 후에 자금을 개방 운영할 경우 〈모델 V〉와 같은 수준으로 안전하다.

☆6 : 특정의 상점 혹은 특정의 이용자에 의한 이중 사용 미수를 검지할 수 있음.

〈표 6〉 발행기관의 정보를 이용한 위조에 대한 분석결과표

			잔고관리형 전자화폐			전자증서형 전자화폐		
암호기술	이용정보 대 상	분석 항목	〈모델 I〉	〈모델 II〉	〈모델 III〉	〈모델 IV〉	〈모델 V〉	〈모델 VI〉
공통키형	본 인	공격 성공 가능성 여부	D_1	A_1	D_1	D_1	A_1	D_1
		공격 성공시 검지 가부	D_2	-	D_2	A_2 ☆7	-	A_2 ☆7
		검지 가능시 대응책 유무	-	-	-	C_3 ☆8	-	C_3 ☆8
	특 정 인	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1	D_1	C_1 ☆9	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	A_2 ☆7	A_2 ☆7	A_2 ☆7
		검지 가능시 대응책 유무	-	C_3 ☆3	-	C_3 ☆8	D_3	C_3 ☆8
	불특정인	공격 성공 가능성 여부	D_1	B_1 ☆4	D_1	D_1	A_1	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	A_2 ☆7	-	A_2 ☆7
		검지 가능시 대응책 유무	-	B_3 ☆3	-	D_3	-	D_3
정적 인증을 요하는 공통키형	본 인	공격 성공 가능성 여부	D_1	A_1	D_1	D_1	D_1	D_1
		공격 성공시 검지 가부	D_2	-	D_2	D_2	D_2	D_2
		검지 가능시 대응책 유무	-	-	-	-	-	-
	특 정 인	공격 성공 가능성 여부	D_1	C_1 ☆1	D_1	D_1	D_1	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	D_2	D_2	D_2
		검지 가능시 대응책 유무	-	C_3 ☆3	-	-	-	-
	불특정인	공격 성공 가능성 여부	D_1	B_1 ☆4	D_1	D_1	D_1	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	D_2	D_2	D_2
		검지 가능시 대응책 유무	-	B_3 ☆3	-	-	-	-
동적 인증을 요하는 공개키형	본 인	공격 성공 가능성 여부	D_1	A_1	D_1	D_1	D_1	D_1
		공격 성공시 검지 가부	D_2	-	D_2	D_2	D_2	D_2
		검지 가능시 대응책 유무	-	-	-	-	-	-
	특 정 인	공격 성공 가능성 여부	A_1	A_1	D_1 ☆6	A_1	A_1	A_1
		공격 성공시 검지 가부	-	-	D_2	-	-	-
		검지 가능시 대응책 유무	-	-	-	-	-	-
	불특정인	공격 성공 가능성 여부	D_1	B_1 ☆5	D_1	D_1	D_1	D_1
		공격 성공시 검지 가부	D_2	A_2 ☆2	D_2	D_2	D_2	D_2
		검지 가능시 대응책 유무	-	B_3 ☆3	-	-	-	-

A_1: 공격불가(매우 안전), B_1: 운용당시 공격방지(다소 안전), C_1: 부분공격 성립(다소 불안전), D_1: 공격성립(매우 불안전)

A_2: 검지가능(매우 안전), D_2: 검지불가(매우 불안전)

A_3: 대응가능(매우 안전), B_3: 상당정도 대응가능(다소 안전), C_3 : 어느 정도 대응 가능, D_3: 대응불가(매우 불안전)

- : 분석불요

☆1 : 도청에 의해 IA'를 입수가능한 A'의 잔고를 탈취할 수 있음.

☆2 : 도난당한 A'(A*)가 자신의 잔고가 감소된 것을 알아채고, 부정 사실을 확인할 수 있음. 또한 센터의 로그에 의해 A'(A*)로부터 어떻게 전자지갑에대해 자금이동이 있었는가를 파악할 수 있음.

☆3 : 부정행위가 이루어진 전자지갑을 거래정지함으로써 피해는 더 이상 발생 불가능함.

☆4 : 임의로 선택한 식별자 I_{A^*}가 실제로 존재하면 A*의 잔고를 탈취할 수 있음.

☆5 : 임의로 작성한 P_{KA^*}, S_{KA^*}가 실제로 존재하면 A*의 잔고를 탈취할 수 있음.

☆6 : 완전한 익명성이 보장되기 때문에 본인을 마치 제3자인 것처럼 위장하여 실질적으로 공격이 성립하는 경우

☆7 : 사후적인 센터 체크에 의해 검지가 가능하며, 부정행위자 및 피해자의 신원 확인이 가능함.

☆8 : 상점이 핫리스트를 입수할 수 있다면 체크가 가능함.

☆9 : 도청(특히 발행시)한 A'의 증서를 미리 사용할 수 있다면 공격이 가능함.

Ⅴ. 결론

지금까지 분석한 결과에 때르면 잔고관리형 전자화폐의 경우 동적 인증을 요하는 공개키형의 암호 방식을 채택한 <모델 Ⅱ>(일방향 폐쇄형·센터관리형·온라인형)가 가장 안전한 전자화폐인 것으로 분석되었다. 그러나 <모델 Ⅱ>가 안전성 면에서는 매우 우월한 전자화폐인 것만은 분명하지만 이것은 현금과 같이 이용자 쌍방간의 자유로운 가치이전(양도성)이 곤란하고 익명성도 떨어지기 때문에 화폐 고유의 기능성이나 효율성 측면에서는 <모델 Ⅲ>(쌍방향 개방형·로칼관리형·오프라인형)이 바람직한 전자화폐라고 생각된다. 그러나 <모델 Ⅲ>의 경우 전반적으로 안전성이 매우 떨어지기 때문에 필히 부정변조에 대한 완벽한 내성 장치가 요구된다.

한편 전자증서형 전자화폐의 경우 발행기관의 정보 보안이 잘 유지된다면, <모델 Ⅴ>(일방향 폐쇄형·로칼관리형·온라인형<즉시검증>)의 경우 정적 인증을 요하는 공개키형이나 동적 인증을 요하는 공개키형의 암호 방식 어느 경우에도 안전성이 보장된다. 그러나 <모델 Ⅳ>(일방향 폐쇄형·로칼관리형·오프라인형<사후검증>)와 <모델 Ⅵ>(쌍방향 개방형·로칼관리형·오프라인형<사후검증>)의 경우는 동적 인증을 요하는 공개키 암호방식을 채택하더라도 안전성이 다소 떨어지기 때문에 부정변조에 대한 내성 장치가 필요하다.

이상의 경우를 종합해 볼 때, 우리 나라의 경우 도입 초기에는 경제적 충격을 최소화하면서 상대적으로 초기투자비용이 적게 들면서 단기간내에 가장 안전하게 사용할 수 있는 <모델 Ⅱ>와 <모델 Ⅴ>과 같은 유형의 전자화폐를 도입하되, 중·장기적으로는 암호기술이나 부정변조에 대한 내성 기술 개발을 통한 안전장치가 보완될 경우 <모델 Ⅲ>이나 <모델 Ⅳ>, <모델 Ⅵ>과 같은 유형의 전자화폐를 상용 결제수단으로 정착시켜 나가야 할 것이다.

향후 연구과제는 전자화폐의 모델 유형별 기술적 한계를 고려하여 모델 유형별로 전자화폐가 도입될 경우 산업별(제조업, 물류·유통업, 금융업), 경제주체별(소비자, 기업, 정부) 영향을 분석하는 일이다.

참고문헌

박재석, "전자화폐의 개발동향과 향후 전망", 정보통신정책, 제9권 제8호(통권 185호), 통신개발연구원, 1997.

신일순, 정보통신보안을 위한 암호체계관련 정책연구, 통신개발연구원, 1996.

오승원, "국내 은행의 전자화폐 추진현황 및 발전능 위한 과제", 『금융』, 1998. 5.

전국은행연합회, "전자화폐시대의 도래와 그 대응방안", 1997.

제일금융연구원, 새로운 돈의 혁명 전자화폐, 한국경제신문사, 1997.

지호준, "전자화폐 개발현황의 국제적 비교와 국내은행의 전략적 과제", 대은경제리뷰, 제191호, 1999.

탁승호, 전자화폐와 경제시스템, 더뱅커사, 1996.

松島克守·中島洋, エレクトロニク·コマースの衝撃, 日本經濟新聞社, 1996.

松本 勉·岩下直行, "金融分野における情報セキ

ュリテイ技術の現狀と課題", 金融研究, 第18卷 第2号, 日本銀行金融經濟研究所, 1999.

岩下直行・谷田部充子, "金融分野における情報セキュリテイ技術の國際標準化動向", 金融研究, 第18卷 第2号, 日本銀行金融經濟研究所, 1999.

宇根正志・岡本龍明, "共通鍵暗號の理論研究における最近の動向," 金融研究, 第18卷 第2号, 日本銀行金融經濟研究所, 1999.

宇根正志・太田和夫, "共通鍵暗號を取りく卷現狀と課題—DESからAESへ—," 金融研究, 第18卷 第2号, 日本銀行金融經濟研究所, 1999.

中山 靑 司・森 秀實・阿部正幸・藤 奇英一郎, "電子マニ-の實現方式にてついて—安全性, 利便性に配慮 した新しい電子マニ-實現方式の提案—", 金融研究, 第16卷 第2号, 日本銀行金融經濟研究所, 1997.

中山 靑司・松本 勉・太田和夫, "電子マニ-を構成する情報技術セキュリテイと安全性評價", 金融研究, 第18卷 第2号, 日本銀行金融經濟研究所, 1999.

八木 勤, 전자상취인[EC]入門, 1996.

Benjamin, R. and R. Wigand, "Electronic Markets and Virtual Value Chains on the Information Superhighway," Sloan Management Review, Winter, 1995.

Boneh, D., R. A. Demillo, and R. J. Liption, "A New Breed of Crypto Attack on 'Tamperproof' Tokens Cracks Even the Strongest RSA Code", 25 Sep.1996. (http//www.bellcore.com/PRESS/ADVSRY96/smrtcrd.html and http//www.bellcore.com/PRESS/ADVSRY96/medadv.html)

Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation, Version 2.0," May 1998.(http://www.radium.ncsc.mil/tpep/library/ccitse/)

Coppersmith, D., C. Holloway, S. M. Matyas and N. Zunic, "The Data Encryption Standard," Information Security Technical Report, Vol.2, No.2, 1997.

Hammer, M. and G.E. Mangurian, "The Changing Values of Communication Technology," Management Review, 1987.

Kalakota, R. & A.B. Whinston, Eelctronic Commerce, Addison-Wesley Publishing Company, Inc., 1996.

_____, Eelctronic Commerce: A Manager's Guide, Addison Wesley Longman, Inc., 1997.

_____, Frontiers of Eelctronic Commerce, Addison-Wesley Publishing Company, Inc., 1996.

Kocher, P. C., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,"(URL:http//www.cryptography.com/timingattack/paper.html, 1995.)

Kocher, P. C., "Differential Power Analysis", (URL:http//www.cryptography.com/dpa/technical/Index.html, 1995.)

National Research Council, Cryptography's Role in Securing the Information Society, 1996.

A Study on Introduction Viladity of the Types of Electronic Money

Jeong-Kyo, Suh*

Abstract

On regarding Problems on information security technology that have its rise in the introduction of electronic money lately, security evaluation of the types of electronic money is important. Therefore in this paper I tried to analyse introduction viladity based on that,in korea. In perticular, there is a synthetical and systematical study on the security of eletronic money, on the viewpoint of choice combination of cryptography technology and the types of attacks on it. And in case of the electronic money that the criterion of efficiency and functionism is superior to that of security, I emphasize on the fact that it could be valid electronic money if it were supplemented by tamper resistance technology in middle-long term

* Division of economics & Business Administration, Joongbu Univ.