전자 지불 시스템의 보안 평가 기준

(Security Evaluation Criteria of Electronic Payment System)

신장균, 황재준(육군사관학교)

Abstract

Recent increase of commercial network integration to World Wide Web(WWW) shifts an ordinary commerce to electronic environment. This draws more people to examine re-assurance of their secure transaction. This study investigates current status of security methodology for Electronic Payment System and extracts important axis of security level for electronic payment. Using these axis as security evaluation criteria, the research proposes a security matrix which consists of four different level of security granularity, hence allowing evaluation of a nation-wide credit card based payment system. Feasible usage of this matrix contributes to security analysis of the electronic system as whole, hence providing better secured electronic environment.

1. 서 론

국내의 전자거래 보안기술은 외국에 비해 매우 취약하며, 보안 프로토콜, 지불 프로토콜, 전자 화폐 시스템 등 3분야 중에서 지불 프로토콜 분야에서만 개발이 이루어지고 있는 상태이다. 국제적으로 대표적인 지불 프로토콜에는 SET(Secure Electronic Transaction)이 있는데, SET 기반의 전자 지불 시스템을 개발하는데는 많은 노력과 비용이 필요하며, 더욱이 개발된 제품의 인증을 받기 위해서 미국의 검사 기관에 많은 수수료를 납부해야 한다. 국제적인 거래가 아닌 국내 전자 거래에 필요한 보안 기술은 SET이 아닌 Non-SET 형태인 독자적 지불 프로토콜을 사용해도 충분하며 실제로 일부 업체에서 Non-SET 기반의 전자지불 시스템을 개발하여 시험 운영하고 있는 중이다. 그러나 공인된 기관에서 적절한 과정을 거쳐 평가된 제품만이 전자거래에 실제로 활용될 수 있으므로 전자 지불 시스템을 보안 특성에 따라 분류하고 보안 기능을 평가할 수 있는 보안 평가 기준과 평가 방법론에 대한 연구가 시급한 실정이다.

본 연구에서는 전자 지불 기술을 분석하고 시스템의 보안 요구사항을 도출하며, 이를 기초로 국내 전자거래에 활용할 수 있는 전자 지불 시스템의 보안 평가 기준을 제시하는데 그 목적이 있다. 제시된 보안 평가 기준은 국내의 전자 지불 시스템을 개발하는데 지침이 될 수 있을 뿐 아니라 향후 전자 지불 시스템의 국제적인 보안 평가 기준 제정 활동에 기여할 수 있다.

2. 전자 지불 기술 분석

2.1 전자 지불 시스템 분류

전자 지불(Electronic Payment)은 컴퓨터 네트워크 환경에서 소비자, 상점, 금융기관 사이에서 발생하는 전자거래 결제의 안전한 처리를 제공하는 기술이다. 전자 지불 관련 정보 보호 기술은 결제수단에 의해 신용카드 기반과 전자 화폐 기반으로 분류할 수 있다. 전자 화폐란 기존의 상거래 결제수단이 아닌 새로운 형태의 결제수단으로서 화폐와 같은 가치를 지닌 디지털 정보를 통칭한다. 신용카드 기반의 전자거래 시스템 구현시 현재 적용되는 기술에는 보안 프로토콜과 지불 프로토콜이 있다. 보안 프로토콜은 인터넷 웹 클라이언트와 서버간에 발생하는 트랜잭션의 비밀성을 보장해 주는 기술로 전자거래 시스템에서 지불 정보에 대한 안전한 전송을 가능케 하는 수단으로 사용되고 있다. 대표적인 보안 프로토콜인 SSL(Secure Socket Layer)은 1993년 웹 서버와 브라우저간의 안전한 통신을 위해 넷스케이프에 의해 개발되어 세션 계층에서 적용된다. 현재 대부분의 전자 쇼핑몰들이 SSL 프로토콜을 지원하는 웹 서버를 구축하고 있으며, 향후 그것의 단순성 및 비용절감 측면을 고려해 볼 때 경쟁력 있는 기술로 고려되고 있다. 1996년 SSL 3.0이 발표된 후, 1998년에는 SSL 3.0이 TLS(Transport Layer Security) 1.0으로 개선된 후 IETF의 표준으로 추진되고 있다. 한편 전자거래의 모든 참여자 간의 발생할 수 있는 트랜잭션을 정의하고 해당 트랜잭션의 안전성 보장을 위한 별도의 프로토콜을 설계함으로써 전체 시스템에 대한 폭넓은 안전성 보장하기 위해 SET(Secure Electronic Transaction)과 같은 지불 프로토콜이 개발되었다. 지불 프로토콜 분야는 SET과 Non-SET으로 분류되며, 국내에서는 SET1.0 사양에 따른 제품 개발이 완료 또는 진행되고 있는 상태이고, 일부 업체들은 자사만의 Non-SET을 개발하고 있는 상황이다. SET은 1996년 VISA와 MasterCard가 주축이 되어 관련업체 지원 아래 개발되었으며, 현재는 SET 1.0이 사용중이고, 향후 개발될 SET 2.0(1999)은 SET 1.0의 기능을 강화·확장시킨 형태로서 스마트카드 및 다양한 암호 알고리즘을 지원할 예정이다. 또한 Non-SET으로는 미국의 CyberCash, First Virtual 등이 있다. 국내의 경우 SET 관련하여 커머스넷 코리아(CNK; CommerceNet Korea)에서 한국형 전자거래 사업을 추진하고 있으며, 데이콤 등이 기술개발을 담당하여 SET 시스템을 구축하고 현재 운영 중이다. 한국과학기술원의 국제전자거래연구센터(ICEC ; International Center for Electronic Commerce)는 메타랜드를 설립하여, SET 시스템을 개발·운영하고

있다. 비씨카드 등 4개 신용카드사와 한국통신 등은 공동으로 코리아 사이버 페이먼트(KCP ; Korea Cyber Payment)를 설립하여 SET 시스템 구축 중이다. Non-SET 관련 이니텍 전자 지불 시스템이 이니텍(주)社에 의해 개발된바 있다. SET 개발에는 많은 비용이 소요되며, 더욱이 개발된 제품의 인증을 받기 위해서는 미국의 검사기관인 SETCo에 많은 수수료를 납부해야만 하는 실정이다. 국내에서 개발된 제품들은 현재까지 SETCo에 인증 신청을 하지 않은 상태이며, 이것은 국제 호환이 아닌 국내에서만 사용 가능하다는 것을 의미한다. SET용 인증기관은 별도로 마스터카드나 비자카드의 인증기관으로부터 인증을 받아야 하며, 그 과정에서 수만불에 이르는 수수료가 요구된다. 이러한 SET 시스템 구축의 어려움으로 인하여, Non-SET 형태인 독자적 지불 프로토콜이 일부 업체에서 개발되고 있으며, 그 예로 강원도청 전자거래 사업에는 이니텍(주)이 참여하여 자사의 지불 시스템을 구축한바 있다. 커머스넷 코리아의 인증기관 서버는 IBM Registry 인증기관 서버를 도입하였고, KCP는 GTE CyberTrust 인증기관 서버를 도입하여 시험 운용 중이다.

한편 전자 화폐 시스템은 가치 있는 디지털 정보를 화폐로 사용하며, 가치 정보는 스마트카드나 컴퓨터의 하드디스크에 저장되는 형태이다. Mondex는 영국의 NetWest 은행의 Tim Jones와 Graham Higgins에 의해 개발되었으며, 1992년 3월 시범 프로젝트를 거쳐, 현재 영국을 중심으로 세계 20여개 국가에서 사용중이다. 스마트 카드 사용 및 암호 기술을 적용한 인터넷 기반이 아닌 오프라인 방식의 전자 화폐 시스템으로서 입출금이 용이하며, 개인간의 계좌이체도 가능하다. 1994년 네덜란드 David Chaum에 의해 DigiCash 회사가 설립된 이후 Ecash 프로젝트가 시작되었고, 1995년 미국의 Mark Twain 은행과 제휴, 인터넷을 기반으로 본격적인 서비스에 돌입한 Ecash는 인터넷 기반의 온라인 전자 화폐이다. Mondex와 더불어 최고의 기술을 가진 전자 화폐 시스템으로 현재 독일, 호주 등의 업체와 연계하여 지속적으로 사업을 확대해 나아가고 있다. 향후 오프라인 방식도 지원할 것으로 예상된다. Mondex는 현재 유럽을 중심으로 폭넓게 사용되고 있으며, 일본 및 호주도 Mondex 시스템을 도입 구축하고 있다. Ecash는 미국의 Mark Twain 은행과 협력하여 전자 화폐 발행 서비스를 제공하고 있으나, 아직까지는 크게 확산되고 있는 상태는 아니다. 일본의 NTT는 1997년부터 전자 화폐 시스템 개발을 추진하고 있으며, 1999년부터 시범 서비스를 예정하고 있다. 국내에서는 금융결제원을 중심으로 은행권, 한국정보통신진흥협회 산하의 "전자 화폐 연구회" 등에서 소규모 연구가 이루어지고 있다. 전자 화폐 시스템은 보안 프로토콜이나 지불 프로토콜과는 달리 웹 기반 기술보다는 스마트카드나 관련 장비에 대한 하드웨어 및 소프트웨어 기술이 요구되며, 국내의 기술 수준은 유럽의 수준과 많은 격차를 보이고 있다. 전자 화폐 시스템의 일종인 소액지불 시스템은 전자 화폐 시스템과 같이 가치를 갖는 디지털 정보를 결제수단으로 사용하나, 센트 또는 센트 미만과 같은 소액거래에 이용 가능하도록 단순한 암호 기술을 활용한 시스템이다. 1996년 9월 미국의 Digital Equipment에 의해 연구 개발된 Millicent는 가장 대표적인 소액지불 시스템이다.

이러한 전자 거래 지불시스템을 결재 수단을 중심으로 분류해 보면 다음 <표1>과 같다.

표 1 전자 지불 시스템의 분류 및 특징

구 분	적용 기술	시스템	특 징
신용 카드 기반 전자 지불 시스템	지불 프로토콜 (SET, Non-SET)	SET : SET 1.0, KCP, CommerceNet	• 상대적 고비용 • 사용이 다소 어려움 • 높은 안정성 (금융기관만 카드 확인) • 금융기관간의 온라인 결제 제공(다자간 협력 필요)
		Non-SET : Cybercash, FirstVirtual, 이니텍	
	보안 프로토콜 (SSL)	Netscape SSL, IE SSL, Apache-SSL	• 상대적 저비용 • 사용이 쉬움 • 낮은 안정성 (상점에 카드번호 노출) • 금융기관간의 온라인 결제 제공 안함(상점 단독 조작)
전자 화폐 기반 전자 지불 시스템	전자 화폐 (스마트 카드, 전자지갑)	Mondex, Ecash	• 오프라인 : - 입출금 용이 - 개인간 계좌이체 가능 - 스마트 카드, 전자서명 등 관련 암호 기술 소요 • 온라인 : 인터넷 기반 - 인출 프로토콜 - 지불 프로토콜 - 예치 프로토콜
	소액 지불 (전자지갑)	Millicent	• 단순 암호기술 소요 (예 : 해쉬함수)

2.2 전자 지불의 보안 요구

안전한 신용카드 기반 전자 지불 시스템의 보안 요구사항에는 기밀성, 인증, 무결성, 암호 알고리즘 및 프로토콜, 상호 운용성, 수용성, 호환성 등이 있다.

(1) 기밀성

지불 정보에 대한 비밀성이 제공되어야 한다. 지불 정보에는 사용자 번호, 사용자 계정 정보, 거래 금액, 거래 내용 등이 포함된다. 또한 주문 정보에 대해서도 비밀성을 보장할 수 있어야 한다. 비밀성은 메시지 암호화를 통해서 이루어진다.

(2) 인증

카드 소지자 및 상점에 대한 안전한 인증이 이루어져야 한다. 이것은 결국 서로간의 상호 인증이 안전하게 이루어져야 함을 의미한다. 인증은 디지털 서명 및 당사자의 인증서를 통해서 이루어진다.

- 카드 소지자의 인증 : 상점이 임의의 카드 소지자가 제시한 지불 카드 계정의 합법적인 사용자인지를 인증 할 수 있어야 한다.
- 상점의 인증 : 카드 소지자가 임의의 상점이 제시한 종류의 지불 카드 거래를 받아들일 수 있는지를 금융 기관과의 관계를 통해서 인증 할 수 있어야 한다.

(3) 무결성

주문 정보 및 지불 정보에 대한 무결성이 제공되어야 한다. 즉, 전송되는 모든 정보의 무결성이 보장되어야 한다. 무결성은 디지털 서명을 통해서 이루어진다.

(4) 암호 알고리즘 및 프로토콜

위와 같이 지불과 관련된 세가지 주요 서비스를 제공하기 위한 암호 관련 알고리즘과 프로토콜이 정의되어야 한다.

(5) 상호 운용성

다양한 판매자들에 의해 개발된 응용 프로그램간의 상호 작용 문제가 해결되어야 하며 서로 상호 운용될 수 있어야 한다. 또한 하부적인 면에서 네트웍 제공자와의 상호 운용성도 고려되어야 한다. 상호 운용성은 특정한 프로토콜과 메시지 포맷을 통해서 이루어진다.

(6) 수용성

하나의 카드 회사가 아닌 다양한 카드회사, 은행 및 상점에서 쉽게 채용될 수 있도록 마련된 표준을 근간으로 한 구현이 필요하다.

(7) 호환성

인터넷상에서 사용되는 다양한 컴퓨터 플랫폼에서 호환성을 가지며 또한 이식성 및 확장성을 가질 수 있도록 표준화된 소프트웨어 개발이 필요하다. 또한 안전한 전자화폐 기반 전자 지불 시스템의 보안 요구사항에는 독립성, 이중 사용, 익명성, 이동성, 분할성, 안전한 기억장소 등이 있다.

(1) 독립성(Independence)

전자 화폐는 주어진 컴퓨터 시스템 또는 장소와는 무관해야 한다.

(2) 이중 사용(Double spending)과 위조 방지

전자 화폐를 재 사용하거나 위조하는 것이 방지돼야 한다. 일반 지폐에 있어서 위조가 있으나 전자화폐에서는 이중 사용이 있다. 지폐에서의 위조는 은행 또는 정당한 발행 기관의 허가 없이 돈을 만들거나 기존의 돈으로부터 새로운 돈을 만드는 행위를 말하지만, 전자 화폐는 전자 정보로 이루어져 쉽게 복사가 가능하다. 1회사용 후 다시 다른 곳에 동일한 전자 화폐를 사용할 수 있다. 지폐에 대한 위조를 방지하기 위해서는 복사하기가 어려운 특수 잉크, 특수 도안 등이 사용되어 위조지폐의 발행을 어렵게 하지만 전자 화폐에 대한

이중 사용 방지는 사용된 전자 화폐의 정보로부터 컴퓨터가 동일한 전자 화폐를 조사하여 이중 사용자의 계좌 번호와 사용자의 신분을 알아내는 방식을 주로 취하고 있다. 온라인인 경우 이중 사용의 방지가 용이하나 오프 라인인 경우 전자 화폐 사용전 거래 중지가 곤란하기에 추후 부정 사용자 방지 대책을 세워야 한다.

(3) 익명성(Anonymity-Privacy)

사용자에 대한 정보나 사용 내역 등은 보호되어야 한다. 즉, 사용자와 상점간의 거래내역, 관계 등은 다른 사람에 의해서 추적될 수 없어야 한다. 사용된 돈으로부터 그 돈의 사용자를 추적불가능하고, 똑같은 계좌에서 두 번의 거래가 이루어져도 두 거래가 똑같은 계좌에서 이루어졌다는 사실을 알 길이 없도록 설계되어야 한다. 이러한 보호는 돈 세탁이나 탈세, 통화 통제 불가능 등의 부정적인 면을 유발하거나 전자 화폐 시스템의 효율을 떨어뜨릴 수 있기에 완전한 익명성의 구현은 신중히 고려되어야 한다.

(4) 이동성(Transferability)

전자 수표는 한 사람으로부터 다른 상대방에게로 쉽게 이동될 수 있어야 한다. 이는 이 돈을 소유한 사람이 사용한 증거를 남기지 않고 발생시켜야 한다.

(5) 분할성(Divisiability)

전자 수표는 액면 금액을 개별적으로 이용가능 해야한다. 예를 들어, 25 디지털 페니는 4 등분의 디지털을 산출할 수 있어야 하고 4개의 4등분된 디지털은 1달러와 같아야 한다.

(6) 안전한 기억장소(Secure Storage)

전자 수표는 고객의 하드 드라이브 또는 PCMCIA 카드와 같은 스마트 카드에 안전하게 저장되는 방법으로 이용 가능해야한다. 더욱이, 인터넷 상에서 다양한 상대방 유형간에 전자 수표를 전송할 수 있어야한다.

3. 지불 시스템의 보안 평가

3.1 정보시스템의 보안 평가 기준

미국은 국방부, NBS(National Bureau of Standards, NIST의 전신) 및 MITRE 등을 중심으로 안전한 컴퓨터시스템의 구축 및 평가 등에 관한 지속적인 연구 결과로 1983년에 소위 "Orange Book"으로 불리우는 안전한 컴퓨터 시스템 평가기준인 TCSEC(Trusted Computer Security Evaluation Criteria) 초안이 제정되었고 1985년에 미 국방부 표준(DoD 5200.28-STD)으로 채택되었다. 미국방부는 안전·신뢰성이 입증된 컴퓨터시스템을 국방부 및 정부기관에 보급하기 위하여 TCSEC을 6가지 등급(C1, C2, B1, B2, B3, A1)으로 분류하여 각 기관별 특성에 맞는 컴퓨터시스템을 도입·운영하도록 권고하고 있다. TCSEC은 보안정책, 표시, 신분확인, 감사기록, 보증 및 지속적인 보호의 기본적인 컴퓨터 보안 요구사항을 갖고 있다. TCSEC을 기초로 선진국들은 자국의 평가 기준을 제정하기 시작하였는데 대표적인 기준에는 유럽 4개국의 ITSEC(Information Technology Security Evaluation

Criteria), 카나다의 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria), 미국의 FC(Federal Criteria)가 있다. 세계 각국의 평가 기준이 상이하여 평가에 소요되는 비용과 시간이 많이 소요되며, TCSEC, ITSEC, CTCPEC, FC 등의 평가기준 통합의 필요성을 절감한 미국(NIST, NSA), 캐나다(CSE), 프랑스 (SCSSI), 독일(BSI), 네덜란드(NL-NCSA) 및 영국(CESG) 등 6개국이 1993년 CC(Common Criteria)를 개발하기로 합의를 하였다. 1998년 5월 버전 2.0이 발표된 상황이며 ISO/IEC JTC1/SC27/WG3에서 표준화를 위한 노력도 병행하고 있다. CC는 크게 5가지 부분으로 구성되어 있는데 Part 1에서는 소개 및 일반모델을 제시하고 있으며 Part 2는 보안기능 요구사항, Part 3는 보증 요구사항, Part 4는 이미 정의된 보호 프로파일을 기술하고 있으며 Part 5에서 보호 프로파일을 등록하는 절차를 포함하고 있다. CC의 핵심은 Part 2와 Part 3로써 정보보호시스템이 구비해야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발할 수 있다.

3.2 전자 지불 시스템의 보안 평가

본 연구에서는 평가 기준 설정의 특성을 고려할 때 전자 화폐 기반전자 지불 시스템은 기준 설정이 부적절하여 연구 대상에서 제외하였으며, 신용 카드 기반의 지불 시스템의 보안 평가에 적용되어야 하는 보안 기능을 아래와 같이 도출하였다.

(1) 신분확인 (Identification and Authentication)

전자 지불 시스템에 접근을 시도하는 사용자가 인가된 사용자인지를 판단하기 위하여 사용자를 식별하고 그 신분을 검증하는 기능과 거래 주체간의 상호 인증 기능

(2) 접근통제 (Access Control)

시스템 보안정책에 의하여 객체에 대한 주체의 모든 접근을 통제하는 기능으로서 임의적 접근통제 및 강제적 접근통제 방법으로 분류

- 임의적 접근통제 (discretionary access control) : 주체가 객체에 접근하려할 때 주체 및 객체의 신분에 기초하여 접근을 제한하는 방법
- 강제적 접근통제 (mandatory access control) : 주체가 객체에 접근하려 할 때 양자의 보안레이블에 기초하여 비밀수준이 높은 객체의 정보가 비밀수준이 낮은 주체에게 유출되지 않도록 접근을 제한하는 방법

(3) 비밀성 (Secrecy)

전자 지불 시스템에서 전송되는 모든 정보의 비밀성이 보장되는 기능

(4) 무결성 (Integrity)

전자 지불 시스템에서 전송되는 모든 정보의 정확성이 보장되는 기능

(5) 부인봉쇄 (Non-repudiation)

전자 지불 시스템을 사용한 거래 주체간에 거래 사실을 부인하지 못하게 하는 기능

(6) 감사기록 및 추적 (Logging and Audit Trail)

전자 지불 시스템의 사용에 대한 증거가 되는 데이터를 시간 순으로 기록·저장하고 이 데이터를 이용하여 사용자의 비 인가된 행위 등에 대한 정보를 조사하는 기능

(7) 증명된 보안모델 (Verified Security Model)

전자 지불 시스템이 보호대상 정보 및 객체를 어떻게 보호 및 관리해야 하는지에 대한 보호 규칙을 명시하기 위하여 정보시스템에 의해 시행되어야 하는 시스템 보안정책을 서술한 모델에서 그 의미가 정확하게 나타나도록 수학적 표기법을 이용하여 서술하는 정형화된 방법으로 증명된 보안 모델

이러한 보안 기능을 기초로 하여 거래 주체간의 상호 인증, 거래 및 지불정보의 비밀 유지, 거래 및 지불정보의 무결성 유지, 거래 공증 서비스, 온라인 분쟁해결, 익명성 제공 여부 등의 수준에 따라 다음과 같이 전자 지불 시스템의 보안 평가 기준을 제시하였다.

등급 D : 최소 보호 전자거래

지불 시스템의 클라이언트(구매자)와 서버(상점)간에 발생하는 트랜잭션의 비밀성을 보장하여 지불 정보에 대한 안전한 전송을 가능케 하며, 클라이언트(구매자)에서 서버(상점) 쪽으로 일방향 인증 기능을 제공하는 보안 등급

등급 C : 안전한 전자거래

거래 당사자(구매자와 상점)간의 상호 인증, 거래 및 지불 정보의 암호화에 의한 비밀성, 전자서명을 통한 무결성, 주체가 객체에 접근하려 할 때 양자의 보안레이블에 기초하여 비밀수준이 높은 객체의 정보가 비밀수준이 낮은 주체에게 유출되지 않도록 접근을 제한하는 강제적 접근통제 (mandatory access control)을 제공하는 보안 등급

등급 B : 인증된 전자거래

거래 당사자(구매자와 상점)간의 상호 인증, 거래 및 지불 정보의 암호화에 의한 비밀성, 전자서명을 통한 무결성, 주체가 객체에 접근하려 할 때 양자의 보안레이블에 기초하여 비밀수준이 높은 객체의 정보가 비밀수준이 낮은 주체에게 유출되지 않도록 접근을 제한하

는 강제적 접근통제 (mandatory access control)을 제공하는 등급 C 기능에 추가하여 안전한 제3자(TTP ; Trusted Third Party)인 인증기관(CA ; Certificate Authority)에 의해 거래 및 지불을 검증하고, 전자 지불 시스템의 사용에 대한 증거가 되는 모든 데이터를 시간 순서로 기록·저장하여 전자 거래 분쟁 해결 기능을 제공하는 보안 등급

등급 A : 증명된 전자거래

등급 B의 보안 기능에 추가하여 전자 지불 시스템의 보안목표 명세서, 기능 명세서, 기본 설계서, 상세 설계서, 보안기능과 보안 모듈에 대한 원시 프로그램 및 하드웨어 도면(하드웨어로 구현한 모듈이 있는 경우), 검증 명세서, 보안모델 명세서가 정형화된 방법으로 기술되어야 하며, 정보시스템의 취약점을 찾아내어 시스템이 제공하는 보안기능을 우회할 수 있는지를 시도해 보는 가능한 모든 침투 시험을 통과한 보안 등급

이와 같은 전자 지불 시스템의 보안 평가 등급의 보안 기능을 요약하면 다음 <표2>와 같다.

표 2 평가 등급의 보안 기능

구분	등급 D : 최소 보호 전자거래	등급 C : 안전한 전자거래	등급 B : 인증된 전자거래	등급 A : 증명된 전자거래
신분확인	△	○	○	○
접근통제	△	○	○	○
비밀성	○	○	○	○
무결성		○	○	○
부인봉쇄			○	○
감사기록 및 추적			○	○
증명된 보안모델				○

4. 결 론

본 연구에서는 전자 지불 시스템의 특성을 분석하고 이를 바탕으로 국내에서 개발되는 시스템의 안정성 수준을 평가할 수 있는 신용 카드 기반의 지불 시스템의 보안 평가 등급을 4단계로 구분하여 제시하였다. 비교적 소액 거래인 경우에는 등급 D(최소 보호 전자 거래)와 등급 C(안전한 전자 거래)의 평가를 받은 시스템이, 또한 고액이고 중요한 전자 거래에서는 등급 B(인증된 전자 거래)와 등급 A(증명된 전자 거래)의 평가를 받은 시스템의 사용이 적절하다. 그러나 전자 화폐 시스템은 지불 프로토콜에 기반을 둔 지불시스템을 보완할 미래지향적 기술로 뛰어난 안전성, 사용의 편리성(온라인 및 오프라인 지원), 사용자 프라이버시 보장 등의 강력한 기능을 제공함으로서 미래 전자 거래 시장의 지불 수단으로 각광받을 것으로 예상되므로 전자 화폐 기반의 전자 지불까지 포함하는 보안 평가 기준의 개발에 대한 연구가 계속되어야 한다.

참고 문헌

[한국전산원98] 전자거래 주요현안 및 대응방안, 한국전산원 CALS/EC 팀, 1998년 6월.

[한국정보보호센터98] 정보통신망 침입차단시스템 평가기준, 한국정보보호센터, 1998년 2월.

[오형근, 이임영99] 전자 화폐 시스템 개발 동향, 한국통신정보보호학회지, 제 9권 제 1호, 1999년 3월

[Anup98] Anup K. Ghosh, E-Commerce Security: Weak Links, Best Defenses, Wiley, 1998.