전자상거래의 계층적 정보보호 메커니즘

한근희*, 박영종**,이봉근**,소우영**
* 한국전자통신연구원, ** 한남대학교 컴퓨터공학과

Hierarchical Security Mechanisms for Electronic Commerce

Keunhee Han*, Youngjong Park**,Bongkeun Lee**,Wooyoung, Soh**
* ETRI, ** Dept. of Computer Engineering, Hannam University

요 약

전자상거래는 인터넷과 같이 보안성이 취약한 개방형 통신망에서 이루어지기 때문에 거래 주체간에 발생하는 거래 정보의 보호를 위하여 기밀성, 무결성, 부인봉쇄 및 인증 등의 정보보호 서비스가 제공되어야 한다. 이러한 문제를 해결하기 위하여 암호 알고리듬 및 전자서명 등이 사용되고 있다. 본 논문에서는 전자상거래 절차를 분석하고 상거래 주체간에 발생하는 정보에 대한 위협요소를 주체별로 분석하여 정보보호 문제를 해결하기 위한 정보보호 메커니즘의 체계적 적용 방안을 제안하고자 한다.

1. 서 론

전자상거래는 전자자금이체, 전자문서교환(EDI)과 같은 전자적인 수단을 통하여 가상공간에서 이루어지는 상거래를 의미한다. 기존의 상거래에서는 일반적으로 일정한 공간에 상점을 개설하고 소비자가 영업 시간 내에 방문하여 물건을 구입한다. 컴퓨터와 정보통신망의 발전으로 기존의 상거래에서도 물류 시스템 및 문서교환 등에서 전자적인 수단을 이용한 형태의 상거래가 실현되고 있다[1]. 현

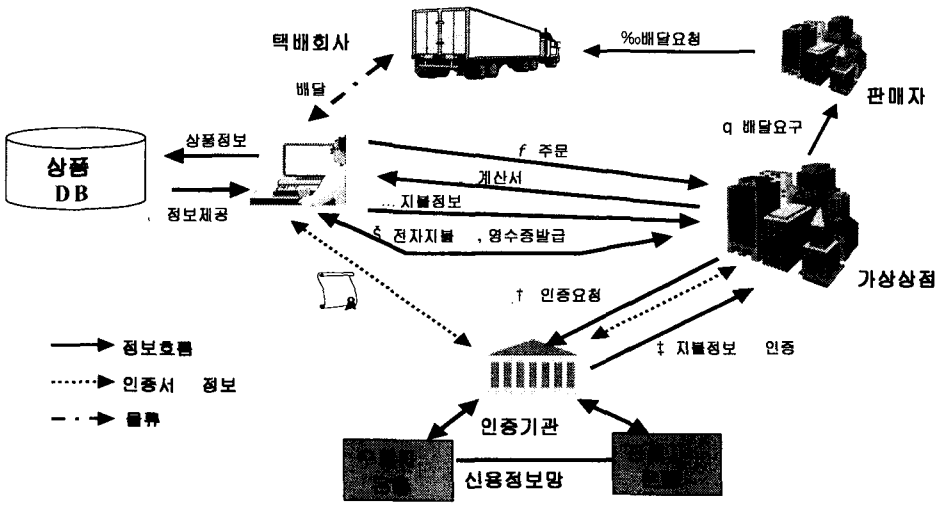
재 전자상거래는 전자문서교환 및 전자자금이체 등의 수단을 확대하여 일반 소비자가 원하는 시간과 장소에서 원하는 물건을 인터넷과 같은 개방형 통신망을 이용하여 구입할 수 있도록 확대하는 추세로 발전되고 있다. 실제로 전자상거래는 부분적으로 물류 EDI, 조달 EDI 등 조직간의 상거래에 사용되고 있으며, 기존의 전자문서교환과 같은 수단을 확장하여 실현할 때 현실적으로 비용 및 안전성 측면에서 유리한 실정이다.

전자상거래는 기존의 VAN EDI를 이용하는 방법과 인터넷을 이용하는 방법이 있으며, 인터넷과 같은 개방형 통신망을 이용하는 경우 거래 정보의 노출, 변조 등과 같은 위협, 거래 당사자간의 신분확인 및 거래사실의 부인과 같은 문제가 발생할 수 있다[2]. 따라서 전자상거래의 실현은 위와 같은 문제점을 해결하는 것이 선결과제다. 본 논문에서는 전자상거래를 기업과 소비자간 모델로 설정하고 판매자, 인증기관 및 택배회사를 포함한 전자상거래 주체들간의 위협 및 문제점을 분석하고, 주체별로 해결 가능한 정보보호 메커니즘의 계층적인 적용 방안을 제시한다.

2 전자상거래 프로세스

주체별 정보보호 메커니즘의 체계적인 적용을 위하여 본 논문에서는 소비자와 기업간의 상거래 절차를 분석하고 상거래 주체간의 정보흐름 및 요구되는 서비스에 대하여 분석하였다. 전자상거래 주체는 소비자, 전자상점, 인증기관, 판매자 및 택배회사로 하였다. 또한 각 거래 절차에서 발생하는 위협요소를 분석하고 필요한 정보보호 서비스와 적용 가능한 정보보호 메커니즘을 제시하였다.

전자상거래는 주체에 따라 소비자와 기업간, 기업과 정부간, 소비자와 정부간 등의 형태로 구분된다. 다음 <그림 1>은 전자상거래 절차를 나타낸 것이며 그 절차와 각 과정에서의 정보보호는 다음 장에서 살펴본다.



<그림 1> 전자상거래 절차

다음 <표 1>은 전자상거래 프로세스에 나타난 정보흐름에 따른 정보보호 서비스 및 메커니즘을 나타낸 것이다.

<표 1> 정보보호 서비스 및 메커니즘

정 보 흐 름	정보보호 대상 정보 정보보호 서비스	정보보호 메커니즘
소비자↔전자상점	물건 주문 정보 기밀성, 무결성, 인증, 부인봉쇄	Web 보안 메커니즘 암호 알고리듬 전자서명
소비자↔인증기관	인증서 정보 기밀성, 무결성, 인증, 부인봉쇄	Web 보안 메커니즘 암호 알고리듬
전자상점↔판매자	물건 주문 내역 기밀성, 무결성, 인증, 부인봉쇄	EDI 보안 메커니즘 암호 알고리듬
판매자↔택배회사	배달 물건 내역 기밀성, 무결성, 인증, 부인봉쇄	EDI 보안 메커니즘 암호 알고리듬
소비자↔택배회사	물류망	ILS(통합물류시스템)
인증기관↔전자상점	소비자 신용 인증 정보 기밀성, 무결성, 인증, 부인봉쇄	EDI 보안 암호 알고리듬
인증기관↔지불기관	지불 신용 정보 기밀성, 무결성, 인증, 부인봉쇄	EDI 보안 암호 알고리듬
지불기관↔판매자	전자 지불 기밀성, 무결성, 인증, 부인봉쇄	Web 보안 메커니즘 암호 알고리듬 전자서명

3. 정보보호 위협요소 및 서비스

3.1 정보보호 위협요소

가. 소비자

소비자는 전자상점 서버의 상품정보를 검색하여 원하는 상품을 전자상점에서 주문하며 상품 인수후 전자상점에게 지불한다. 소비자는 지불과정에서 인증기관으로부터 자신의 인증서를 발급 받는다. 주문은 소비자가 원하는 상품을 선택하여 전자상점에 알리는 일이며, 대부분의 전자상점에서는 주문 시 소비자가 지불수단과 배달방법 등을 선택할 수 있도록 한다. 소비자가 미리 지정된 양식 등에 필요한 항목을 채워 넣거나 표시하여 전자상점으로 보내면 주문이 이루어진다. 이와 같은 소비자의 주문작업에는 전자양식 등을 사용하며, 주문서를 전자상점에 전자우편(E-mail)을 이용하여 전달한다. 소비자가 전송한 거래정보는 인터넷을 통하여 전자상점에 전달된다. 인터넷은 개방형 통신망이기 때문에 IP spoofing 이나 Packet sniffing과 같은 내재되어 있는 취약점이 있다[4]. 따라서 전자상점에서 제공되는 상품정보, 거래 정보 및 개인의 신상정보의 노출 및 변조로 인한 개인정보보호 문제와 재산권 침해 문제 등이 발생할 수 있다.

나. 전자상점

전자상점은 물건에 대하여 불특정 다수의 구매자에게 광고를 통하여 알린다. 소비자가 검색 엔진 및 도구를 통하여 원하는 제품이나 서비스를 제공하는 전자상점 혹은 판매자를 찾을 수 있도록 해야 하며, 판매자는 소비자가 원하는 제품이나 서비스를 찾는 데 소요되는 시간과 비용을 최소화 할 수 있어야 한다. 시간과 비용을 단축시키기 위해서 구매자와 판매자는 검색로봇과 같은 지능형 에이전트 기능을 이용할 수 있다. 소비자는 웹 브라우저 상에 나타난 텍스트, 이미지, 사운드를 비롯한 동영상 등 다양한 형태로 제공되는 멀티미디어 데이터의 전자카탈로그를 이용하여 쇼핑을 하게 된다. 또한 제품의 기능 및 성능을 구매자가 직접 확인할 수 있도록 하기 위한 데모도 가능하여야 한다.

전자상점은 거래 정보 및 상품정보를 저장하고 있기 때문에 전자상점 시스템에

대한 시스템 보안이 요구된다. 시스템 보안은 내부의 자료의 노출 및 변조 등이 있을 수 있으며, 시스템 내부 사용자의 정보 남용과 같은 위협요소가 존재한다. 시스템 보안은 방화벽과 같은 도구를 통하여 해결하고 있으나, 내부 사용자의 정보 남용은 막을 수 없기 때문에 침입탐지기술 등이 요구된다.

다. 인증기관

전자상거래에서는 전자적인 형태의 문서를 거래 주체간에 주고받는다. 전자문서는 특성상 위조 및 변조의 위험성이 존재하므로 거래내역에 대한 증명을 해줄 제 3의 기관이 요구되며, 공개키의 정확성을 보장하기 위해서 제안된 것이 인증기관이다.

기존의 상거래에서 상거래 주체간의 신분 확인은 직접 만나서 하기 때문에 문제가 되지 않지만 전자상거래에서는 상거래가 사이버공간상에서 이루어지기 때문에 상거래 주체간의 상호 신분 확인 및 거래 사실의 부인 봉쇄 기능이 요구된다. 따라서, 인증 기술은 전자상거래의 핵심 기술이 된다. 인증기관은 SET을 기반으로 하는 인증 체계와 MISSI를 기반으로 하는 인증 체계가 있다[3].

3.2 정보보호 서비스

전자상거래에서 주체간의 위협요소를 해결하는 데 필요한 정보보호 서비스는 다음과 같다.

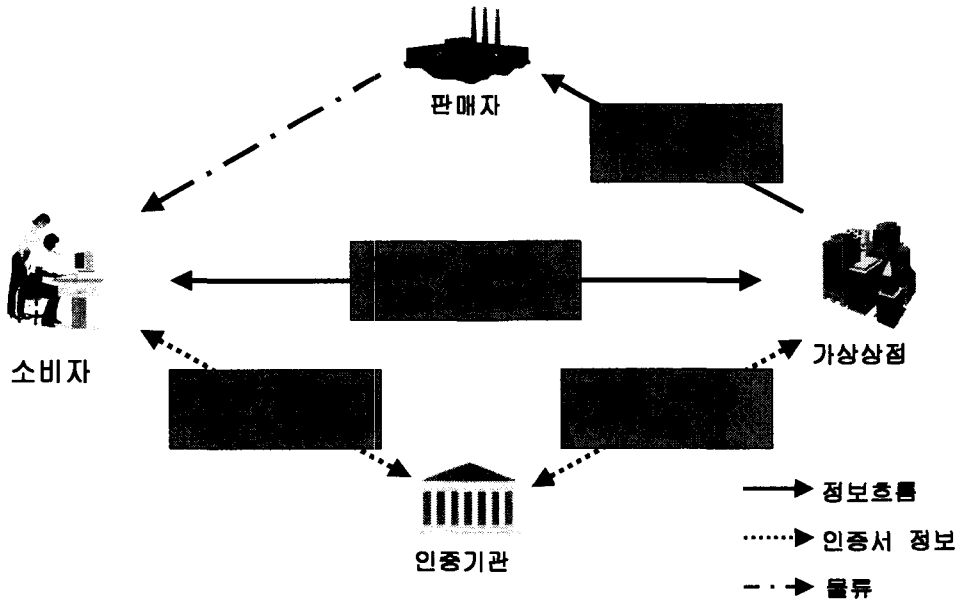
소비자는 구매시 물건의 수량과 가격에 대하여 합의를 통하여 주문한다. 주문은 가상공간상에서 이루어지기 때문에 전자적인 문서로 행해진다. 전자적 주문서를 거래하는 경우에는 주문서의 기밀성과 무결성, 인증 및 부인봉쇄를 위하여 메시지를 암호화하고 소비자의 전자서명을 첨부하는 것이 필요하다.

전자상점은 소비자에게 인터넷을 통하여 24시간 원하는 정보를 제공할 수 있어야 하며, 소비자가 구매시 대금 결제를 위하여 인증기관을 통한 사용자 인증 및 주문접수 내용에 대한 부인봉쇄 등의 기능을 제공하여야 한다. 또한 전자상점에서 소비자의 주문서를 처리하는 방법은 전자상점의 운영정책 등에 따라 다를 수 있으나, 전자상점 측면에서는 운영정책 수립의 유연성을 확보할 수 있도록 다양

한 정보기술을 제공하여야 한다. 전자상점 내에서 주문처리를 위해서는 전자상점과 판매자, 전자상점과 은행과의 자료교환 등 전자상점과 외부기관과의 정보교환이 필수적이므로, 메시징 기술인 전자자료교환, 전자우편 등이 활용될 수 있다.

인증기관은 거래 주체 상호간에 발생하는 거래 정보의 인증, 무결성, 부인방지 등을 제공하기 위하여 거래 주체간의 공개키의 정확성을 보장하는 제 3의 기관을 의미한다. 즉, 공개키의 정확성을 보장하기 위해서 제안된 것이 인증기관이다[5].

소비자의 물건 대금을 지불하는 전자지불시스템의 보안은 매우 중요하며 그 기능으로는 현금 대체 기능, 정보 저장능력과 안전정 및 편리성 등이 요구된다. 기존의 신용카드 기반의 지불수단으로는 Visa와 Master사에서 공동으로 개발한 SET가 있으며, 현재 전자 지불시스템은 크게 IC 카드 기반형과 네트워크 기반이 있다[6]. <그림 2>는 전자상거래시 주체간 요구되는 정보보호 서비스에 대하여 나타낸 것이다.

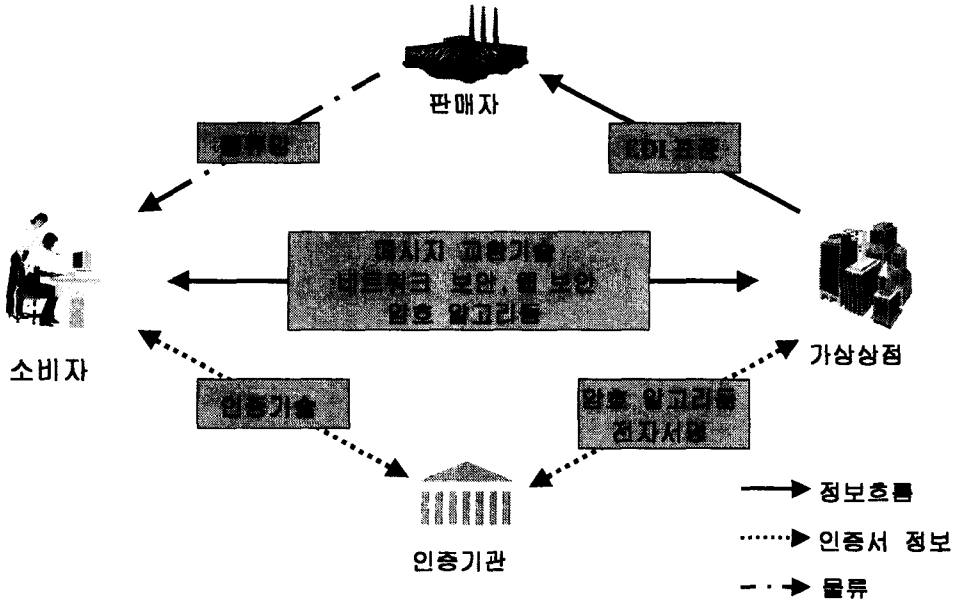


<그림 2> 전자상거래 주체간의 정보보호 서비스

3.3 정보보호 표준화 기술

전자상거래에 주체간의 요구되는 정보보호 서비스를 분석하였다. 안전한 전자상거래를 위해서는 전자상거래 주체간의 위협요소를 해결할 수 있는 정보보호 서비스가 제공되어야 하며, 정보보호 서비스를 해결할 수 있는 정보보호 메커니즘의 적용이 요구된다.

<그림 3>은 전자상거래 주체간의 정보보호 표준기술을 나타낸 것이다.



<그림 3> 정보보호 표준 기술

소비자와 전자상점간의 거래정보 보호를 위하여 적용되는 메시지 교환기술은 X.400, X.435, SMTP/MIME, PGP, PEM 및 S/MIME 등과 같은 EDI 전송표준인 MHS(Message Handling System)와 전자우편 보안 메커니즘 등이 사용된다[2].

암호 알고리듬은 대칭 암호인 DES와 비대칭 암호인 RSA 등이 사용되며, 인증표준은 공개키 기반의 PKIX와 X.509를 사용한다. 메시지 교환 기술과 암호 알고리듬을 통하여 네트워크 보안 기술을 제공한다. 또한 웹 보안 기술표준은 SSL, SHTTP 등이 사용된다. 전자상점과 인증기관 사이는 인증 정보를 교환하며 암호 알고리듬, 전자서명을 통하여 정보보호 서비스를 제공하며, 인증기관과 소비자 사

이에는 상거래시 소비자의 신용정보를 알 수 있는 인증서 정보를 교환한다. 인증기관에서 사용되는 정보보호 표준 기술은 PKI(Public Key Infrastructure)를 기반으로 하며, 신뢰성 있는 인증을 위하여 인증 체계는 계층적 또는 네트워크 형태가 사용된다[5].

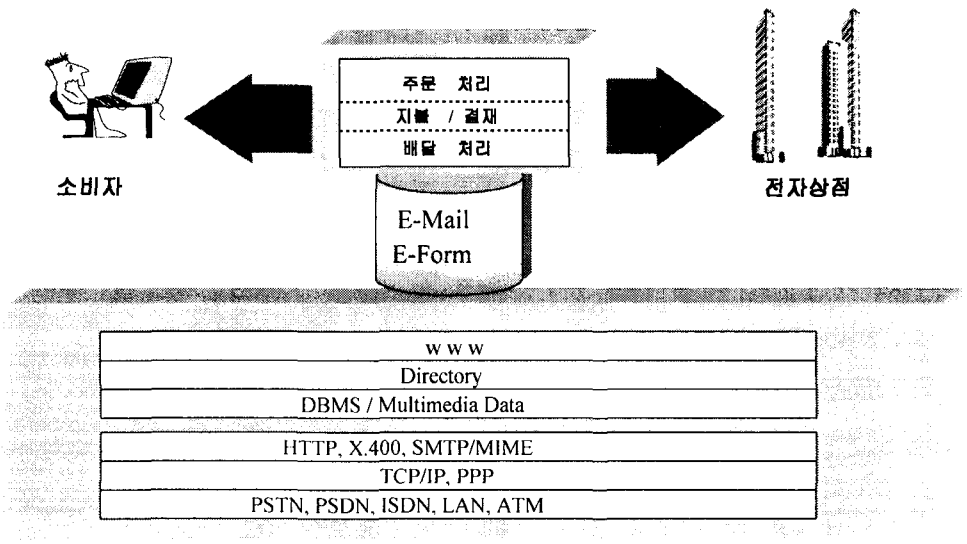
4. 정보보호 메커니즘의 적용

4.1 정보보호 메커니즘

전자상거래 적용기술을 계층적으로 분류하여 하부구조인 통신망기술부터 소비자가 직접 사용하는 웹 환경의 웹 보안까지 각 계층별로 나와 있는 기술구조를 보면 통신망기술은 PSTN, PSDN, ISDN 등이 사용되며 상부 계층에서는 각 계층별로 EDI의 기본 서비스인 X.400, X.435 등을 사용하고 있으며, 거래 정보의 교환은 기본 EDI, E-mail 보안서비스를 적용한다.

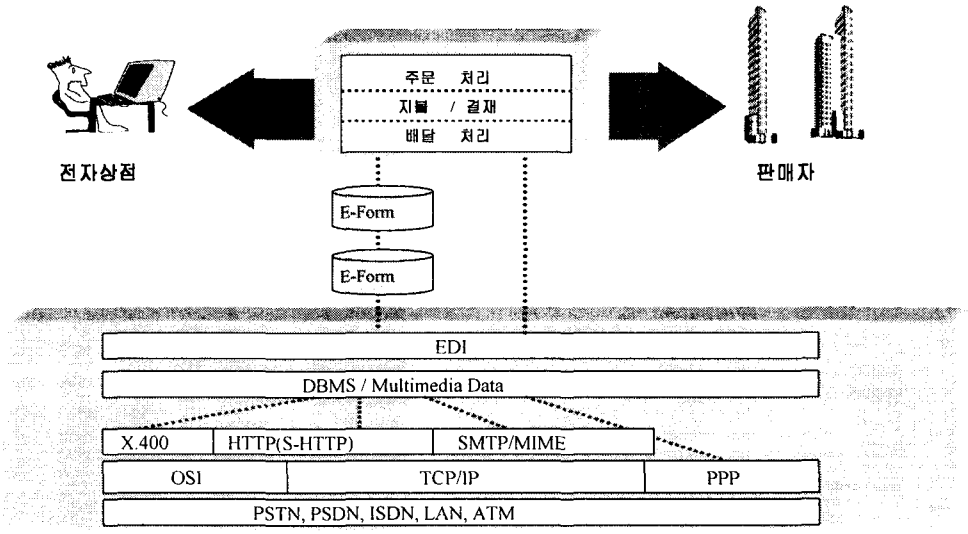
전자상점은 소비자에게 상품정보를 전자카탈로그를 제공하기 위한 멀티미디어 기술, 상품정보의 광고, 검색을 위한 효율적인 검색도구의 개발 및 효율적인 지불시스템의 개발 등이 요구된다. 웹 보안기술은 현재 웹 브라우저는 기본적인 인증기능을 제공할 뿐 세부적인 기밀성, 무결성 및 인증 등을 제공하지 않기 때문에 별도의 S-HTTP, SSL 등과 같은 보안 메커니즘이 제공되어야 한다.

소비자와 전자상점간에는 인터넷을 기반으로 하는 전자우편과 같은 수단을 통하여 상거래 정보를 교환하기 때문에 전자우편 보안 메커니즘이 요구된다. 다음 <그림 4>는 소비자와 전자상점간의 정보보호에 필요한 정보보호 메커니즘의 구성을 나타낸 것이다.



<그림 4> 소비자와 전자상점간의 자료교환

가상상점과 판매자간에는 인터넷 EDI와 같은 수단을 통하여 상거래 정보를 교환하기 때문에 기존의 EDI 보안 메커니즘이 요구된다. 다음 <그림 5>는 가상상점과 판매자간의 정보보호에 필요한 정보보호 메커니즘의 구성을 나타낸 것이다.

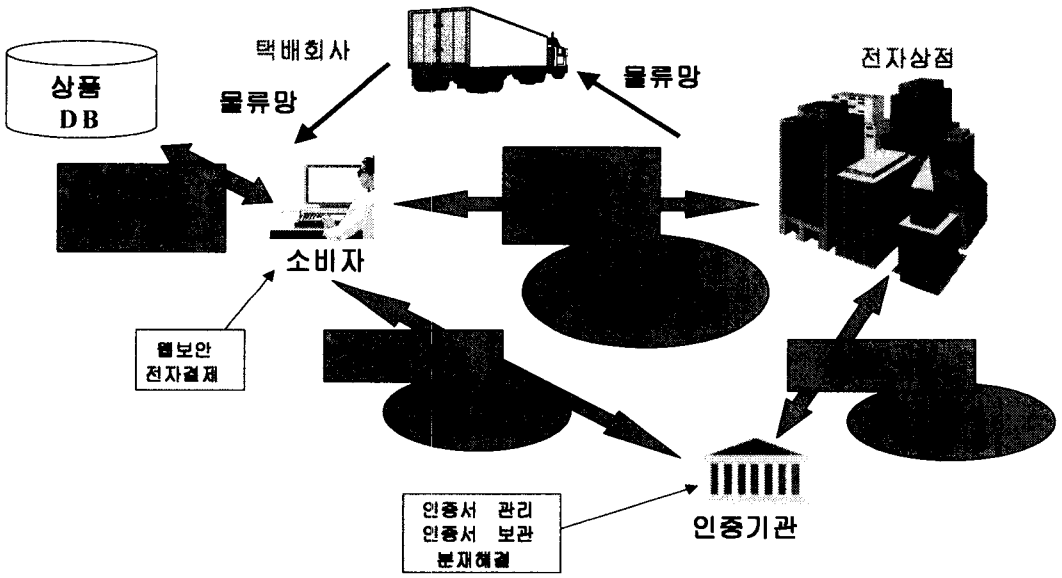


<그림 5> 전자자료교환

4.2 전자상거래 개념 모델

본 논문에서는 소비자와 기업간의 전자상거래에서의 정보보호 위협요소 및 기

술구조를 분석하였다. 전자상거래 주체는 소비자와 기업을 포함하여 거래 당사자의 거래 사실을 확인해주기 위한 인증기관 및 대금지불을 위한 지불 대행기관이 참여 주체가 된다. 소비자와 전자상점간에는 인터넷과 같은 개방형 통신망의 전자우편과 같은 방법을 통하여 주문서를 비롯한 거래정보의 교환이 이루어지기 때문에 전자우편 보안 기술, 웹 보안 메커니즘의 적용이 요구된다. 또한, 전자상점과 판매자 또는 인증기관 사이의 정보 교환은 인터넷 EDI 기술과 EDI 보안 기술 등이 적용된다. 다음 <그림 6>은 전자상거래 주체별 정보보호 서비스와 메커니즘을 적용한 전자상거래 개념 모델을 나타낸 것이다.



<그림 6> 전자상거래 개념 모델

소비자와 전자상점간의 위협요소는 네트워크 상에서의 거래정보의 노출 및 변조, 전자상점시스템 보호, 거래 사실의 상호 인증 등이며, 요구되는 정보보호서비스는 기밀성, 무결성, 인증, 부인봉쇄 등이며 적용 메커니즘은 암호 알고리듬, 메시징 표준, 전자 서명 및 전자 인증서 등이다.

소비자와 지불기관사이에는 지불정보 및 소비자의 현금정보에 대하여 보호가 이루어져야 한다. 요구되는 정보보호 서비스는 기밀성, 무결성 및 부인봉쇄 등이

며, 적용 메커니즘은 웹 보안 메커니즘과 암호 알고리듬이다.

전자상점과 인증기관 사이는 소비자의 신용정보를 주고 받기 때문에 신용정보의 노출 및 변조 등이 있을 수 있다. 요구되는 정보보호 서비스는 기밀성, 무결성 및 부인봉쇄 등이며 암호 알고리듬, EDI 보안 메커니즘 등이 적용된다.

5. 결 론

현재 전자상거래는 선진 각국이 자국의 이익을 위하여 주도적으로 확산시키고 있으며 우리 나라도 이에 적극적으로 대응해야 할 것이다. 전자상거래의 효과적인 실현을 위해서는 정부차원의 정책수립, 법률 및 제도 정비, 국민 개개인의 마인드 확산, 요소 기술 개발 및 초고속 통신망과 같은 기반 환경 조성 등이 복합적이고 유기적으로 추진되어야 한다. 또한, 인터넷과 같은 개방형 통신망을 통한 전자상거래는 거래 정보의 노출 및 변조 등에 대한 취약성과 개인 정보보호의 문제를 안고 있어 거래 정보의 보호 문제가 중요한 선결 과제이다.

본 연구에서는 소비자와 기업간의 전자상거래에서 발생할 수 있는 정보보호 위협요소를 주체별로 분석하고 주체간의 정보흐름과 기능을 분석하여 기존의 정보보호 메커니즘을 체계적으로 적용한 전자상거래 개념 모델을 제안하였다. 제안된 개념 모델은 정보보호를 위한 세부적인 설계 및 구현 과정을 통하여 검증되어야 할 것이며, 본 논문에서 분석된 전자상거래 구현 시 고려되어야할 각 주체별 위협요소, 거래 주체간의 정보 흐름에서 제공되어야 할 정보보호 서비스, 거래 주체의 기능 및 특성에 따라 적용될 수 있는 정보보호 메커니즘 및 정보보호 메커니즘의 적용 기준 등이 활용될 수 있을 것이다.

*. 참고문헌

1. 임춘성 외 3, "전자상거래 구현을 위한 기술 체계와 적용요인 분석", 한국 CALS/EC 학회지 제2권 제2호, 1997. 12.
2. 고승철, 성맹희, "정보보호 기술 분류", 정보처리지 제4권 제2호, 1997. 3.
3. 고영철 외 3, "SET을 기반으로 한 전자상거래 트랜잭션 모델링에 관한 연

구", 한국 CALS/EC 학회지 제2권 제1호, 1997. 6.

4. 김기현 외 3, "정보보호 기술 분류", 통신정보보호학회지 제8권 제1호, 1998. 3.

5. 김종기, "미 국방부의 다수준 정보체계보안사업(MISSI)", 정보처리지 제4권 제2호, 1997. 3.

6. 정준원 외 3, "전자지불시스템 기술 및 표준동향 분석", 정보처리지 제5권 제2호, 1998, 3.