인터넷 전자거래의 기술동향

인터넷(Internet)은 세계 최대의 공공 전산망이다. 즉 약 5만개의 네트워크가 결합되어 있으며 여기에는 약 400만대의 주전산기가 연결되어 각종 정보를 제공하고 있다. 이러한 인터넷은 정보의 산실로서 약 5,000만명의 사용자가 이를 이용하고 있다. 인터넷의 성장세는 연 100%를 능가하며, 가히 폭발적인 증가를 하고 있다. 〈편집자 주〉

김 종 률 동성정보통신(주) 이사

인터넷은 TCP/IP 프로토콜을 사용하고 있으며 윈도우, 매킨토시를 위시하여 각종 유닉스 기종까지 멀티플랫폼을 지향하고 있고 웹브라우저 등 시장 표준화된 단말기를 이용하므로 전세계 어느 곳에서나 용이하게 접속하여 편리하고 신속하게 사용할 수 있다. 인터넷의 대표적인 활동분야인 월드와이드웹(WWW)을 이용한 정보검색 그리고 전자메일서비스 외에도, 인터넷 가상뱅킹, 인터넷 전자상거래 그리고 인트라넷구축 등의 상업적 활용분야가 있다.

인터넷 가상뱅킹서비스는, (1) 날로 현금취급비용이 증가하고 있고 고객들의 금융서비스 다양화요구에 부응해야 하고 초고속 정보통신망 등 정보통신망 환경에 변화에 따라 비금융권 즉 통신회사, 전화회사, 부가정보서비스회사 등의 금융관련서비스가 확대되는 등 금융환경의 변화에 대처하고, (2) 전산 및 정보통신장비의 하락과 인터넷기술 및 보급이 늘고 있고 암호화기술이 발전하는 등 기술환경이 변화하고 있고, (3) 사회기반구조가 산업화사회로부터 정보화사회로 변화하는 등 사회환경의 변화에 따라 출현하게 된 것이다.

이에 따라 고객은 금융거래를 위해 은행이나 자동화기기를 찾아가는 시간이 단축됨은 물론 시간과 공간의 제약으로부터 벗어나게 되고, 은행은 현금출납업무 등 창구업무가 감소되어 인건비와 영업점개설에 필요한 비용감소로 원가의 절감을 얻게됨과 동시에 차별화된 다양한 신상품서비스가 가능해 진다.

강화되는 안전위한 보안기술

인터넷과 같은 온라인 통신상에서 보안의 역할은 아무리 강조해도 지나치지 않다. 특히 인터넷 가상은행이나 전자상거래와 같이 금융관련 업무에서는 송수신 자료보안이 특히 중요하다. 즉 통신 상대방 및 내용이 정확하게 확인되어야 하고, 정보 송신자와 수신자 사이의 책임범위를 명확히 하여 상호간의 부인방지가 이루어져야 한다. 그리고 주고받는 메시지에 대해서 제3자에 의한 불법사용이나 해독으로 인한 프라이버시 침해가 방지되어야 한다.

DES는 Data Encryption Standard의 약자로서 IBM에서 개발하여 1977년 미국정부에 의해서 암호화표준기술로 공식선정된 바 있다. DES는 세계에서 가장 널리 알려져 있고 사용되는 암호화기술이다. 대칭적인 알고리즘으로 단일 비밀키를 사용한다. 항간에 DES가 깨졌다는 말들이 오가고 있으나 사실이 아

니다. 즉 이론적이고 학술적인 얘기일 뿐이고 현실적으로는 그렇지 못한 것이다. DES에 대한 공격은 2의 55승이라는 천문학적인 반복계산에 의하여 만이 가능하여 여기엔 현재기준 약 일백만달라라는 거액의 비용이 소요된다. DES의 보안성을 유지하기 위해서는, 자주 키값을 변경하거나 이중 혹은 삼중암호화를 하거나 RSA와 같은 비대칭 암호화기술과 적절히 혼합하여 사용하면 된다. RSA는 공개키방식의 암호화 및 인증용 암호화기술이다. RSA라는 이름은 Rivest, Shamir, 그리고 Adleman등 창안자 세사람 이름의 머릿글자로부터 지어진 것이다.

RSA는 공개키(Public Key)와 비밀키(Private Key) 한쌍으로 구성되어서, 전문이 공개키에 의해서 암호화되어 비밀키에 의해서 복호화되거나 또는 전자서명의 경우와 같이 전문이 비밀키에 의해서 암호화되어서 공개키에 의해서 복호화된다. RSA의 계산은 DES에 비해 복잡한 편으로서 소프트웨어에서 실행할 때, DES에 비해 적어도 100배의 시간이 소요되며 각기 적절한 하드웨어에서 실행될 때는 적어도 1,000배의 시간이 소요된다. 이와같은 암호화기술을 적절하게 사용하여 인터넷 전자상거래 상에서 안전하게 고객, 가맹점, 은행 등의 가입주체 사이에 거래전문을 주고받을 수 있도록 비자인터내셔널과 마스타카드는 SET(Secure Electronic Transactions)라는 인터넷거래 보안사양을 발표했다.

여기에 참여한 업체는 GTE, IBM, 마이크로소프트, 넷스케이프, SAIC, 테리사 그리고 베리사인 등이다. SET에서 송신자측 컴퓨터에서의 처리절차를 요약하면 다음과 같다. (1) 전문은 정해진 단방향 해쉬함수에 의하여 요약문(Message Digest)을 전환되고 (2) 이는 다시 송신자 서명용 비밀키(Private Key)에 의해서 암호화된다. 이를 전자서명(Electronic Signiture)이라 한다. (3) 원래의 전문과 전자서명은 난수발생방식으로 임시생성한 DES용 대칭키를 이용하여 암호화한다. (4) 앞서 사용된 DES용 대칭키를 수신자 키교환용 공개키(Public Key)를 이용하여 암호화한다.

이를 전자봉투(Digital Envelop)라 한다. 송신자는 (3)과 (4)의 결과를 수신자에게 전송한다. 수신자는 우선(1) 전송된 전자봉투를 수신자 키교환용 비밀키(Private Key)를 가지고 복호화하여 DES용 대칭키를 얻어낸다. (2) 이를 가지고 전송된 암호문을 DES에 의하여 복호화해서 원래의 전문과 전자서명을 얻어낸다. (3) 원래의 전문은 정해진 단방향 해쉬함수에 의하여 요약문(Message Digest)으로 전환된다. (4) 전송된 전자서명은 송신자 서명용 공개키(Public Key)에 의하여 복호화된다. 즉 요약문(Message Digest)을 얻는다.

이 결과는 (3)의 결과와 비교하여 동일함을 확인한다. 이러한 절차에 따라 거래전문을 주고 받음으로써 제3자에 대한 전문내용의 보안이 보장되고 송신자 및 수신자간의 내용 및 본인확인이 가능해진다. 추가될 사항으로는 각자의 공개키(Public Key)에 대해서 권위있는 공공기관(CA)에 의한 키등록 및 인증에 대한 부분이다 현재 인감등록 및 인감증명의 발급을 국가기관에서 하고 있는 것과 같이 상기 공개키에 대해서도 하루빨리 국가기관에 의한 등록 및 증명발급이 전산망상에서 이루어져야 할 것이다.

또 한가지는 고객 등 송신자측의 비밀키(Private Key)의 보관방법이다. RSA는 키는 128비트에 이르는 헥사값으로써 노트에 적어두거나 PC등의 하드디스크에 보관하기에는 너무도 위험하기 때문에 이에 대한 보완책 마련이 시급하게 대두되고 있다.

IC카드와 네트워크 시스템간 결합

인터넷을 기상은행, 전자상거래 등 상업적으로 활용하는 데에 있어서 가장 중요한 점은 가치의 안전하고 편리한 전달방법이다. 따라서 전자화폐의 개념이 등장하게 되었다. 전자화폐란 일렉트로닉 머니(Electronic Money), 사이버 머니(Cyber Money), E-캐쉬(E-Cash), 버추얼 커런시(Virtual Currency), 디지털 캐쉬(Digital Cash), 그리고 스마트 머니(Smart Money)등으로 불리기도 한다. 전자화폐의 특징은 : (1) 통신기능, 즉 전산망을 이용하여 국내외의 원격지에 전자화폐를 직접 보내고 받을 수 있다. (2) 휴대기능, 부피가 큰 잔돈이나 여러가지 지폐를 준비할 필요없이 전자지갑에 넣어 가지고 다닐

수 있다. (3) 대화기능, 전산망에서 지불방법이나 이용방법을 선택할 수 있다. (4) 교환기능, 일일이 현금으로 교환할 필요없이 정확한 환율정보에 의하여 전자적으로 이체하거나 환전할 수 있다. (5) 관리기능, 사용내역 및 정보가 간단히 집계되므로 계획적인 지출생활이 가능하다는 것 등이다.

이러한 전자화폐를 안전하게 보관하고 휴대할 수 있는 수단을 제공하는 것으로 IC카드 또는 스마트카드가 있다. IC카드는 자체연산기능과 내부자료기능이 뛰어나서, 여러가지 기능을 한장의 카드에 넣어 복수의 서비스를 받을 수 있다. 예를 들어서 한장의 IC카드의 개인정보 및 보안정보, 전자통장, 전자지갑, 신용카드, 직불카드, 도서대출카드, 주민등록증, 의료보험증, 운전면허증 등 각종 면허증, 출입통제용키 그리고 각종 쿠폰이나 티켓, 토큰 등을 상호독립적으로 수록하여 별도의 목적으로 사용할 수 있다. 따라서 IC카드와 인터넷 등 네트워크시스템간의 결합은 세계적인 경향으로서 급속하게 진행되고 있다.

인터넷 전자상거래 솔루션을 경쟁적으로 개발추진하고 있는 미국의 이 분야의 거대기업인 마이크로소프트사와 넷스케이프사는 각자 관련기업과 개발그룹을 결성하여 IC카드를 인터넷거래의 보안 및 가치저장수단으로 사용하기 위해 대대적인 노력을 경주하고 있다. 마이크로소프트사는 불란서의 불(Bull CP8)사, 미국의 HP사 불란서의 슐럼버저(Schlumberger)사, 지멘스 닉스도르프(Siemens Nixdorf) 정보시스템사 등 5개사로 이루어진 PC/SC 워킹그룹을 1996년 5월 결성하고, 스마트카드를 연결한 인터넷거래 보안솔루션을 금년내 상용화한다는 목표하에 개발중이며, 넷스케이프사는 베리사인(Verisign)사, 리트로닉(Litronic)사, 컨센서스(Consensus)사, HP사와 손잡고 IC카드를 이용한 인터넷 보안시스템인 SNAPI(Security Native API)의 개발추진을 1997년 2월 RSA 컨퍼런스에서 발표했다.

한편 동성정보통신에서도 인터넷을 비롯한 네트워크환경에서 단말기의 IC카드와 서버를 직접 연결하여 인트라넷, 가상뱅킹, 그룹웨어 등의 단말기보안을 획기적으로 강화시킬 수 있고 전자화폐를 IC카드에 저장하여 전자상거래나 가상은행거래시 직접적인 온라인 전자화폐 대금결제가 가능한 네트워크-IC카드 연결 엔진인 사이언스(SCIENCE : Smart Card Interface Engine for Network Client Environment)를 국내에서 독자적으로 개발하여 1996년 9월 발표한 바 있다.

네트워크와 IC카드가 연결됨으로써 사용자인증에 의한 단말기보안이 강화될 뿐만 아니라, 전산망에서만 존재하고 온라인 처리만이 가능한 이른바 '네트워크형 전자화폐'가 IC카드를 이용한 '가치저장형 전자화폐'와 통합되게 되어 오프라인 처리까지도 가능해진다. 즉 가상은행서비스에서 IC카드의 전자지갑 기능을 이용하여 은행계좌로부터 전자화폐를 인출 또는 예금서비스를 제공할 수 있으며, 전자상거래에서는 전자지갑으로부터 즉시 대금결제를 수행할 수 있어서 이른바 '전산망을 통한 현금거래'가 가능해진다.

한편 개인이 전산망의 정보서비스 접속시점에 암기하여 입력하여야 할 각종 개인관련 고유번호, 암호, 기타자료 등을 IC카드에 수록함으로써 일일이 매번 입력하여야하는 불편함이 없어진다. 특히 비자와 마스타카드의 보안거래절차인 SET(Secure Electronic Transaction)의 경우, 개인 비밀키(Private Key)를 안전하게 보관하는 것이 관건인데 현재로서는 IC카드가 유일하고 최선인 방법인 것으로 전망된다.

그리고 사용자단말기에 IC카드가 연결되어 있으므로 정보서비스 서버는 이 IC카드에 거래량 누적포인트, 할인쿠폰, 예매티켓, 토큰 등을 원격지에게 직접 기록해 줄 수 있어서 이 카드를 휴대한 고객은 해당되는 서비스가맹점의 오프라인 단말기를 통하여 다양한 서비스를 편리하게 제공받을 수있게 된다.

국내의 경우 이미 30여만장의 금융권 IC카드가 보급되어 있고, 1998년에는 전국민을 대상으로한 전자주민카드가 발급될 예정이며, 비자, 마스타카드를 비롯한 신용카드사의 전자지갑카드와 한국은행을 중심으로한 국내 금융기관 IC카드가 보급될 전망인데, 이러한 IC카드가 급속하게 확산되고 있는 인터넷, PC통신, 그리고 그룹웨어 등 전산망시스템과 직접 연결됨으로써, 양대분야가 결합한 새로운 형태의 정보서비스시대로 나아가는 획기적인 전환점을 맞이하게 될 것이다.