「經營情報硏究」 第4號
大韓經營情報學會
2000年 6月

전자상거래상에서의 정보보호 위협요소 분석에 관한 연구

강 석 주* · 김 창 태**

〈목 차〉

Ⅰ. 서 론

컴퓨터 및 정보통신기술의 발전과 더불어 전세계적으로 급속히 확산되고 있는 인터넷 및 초고속통신망을 이용한 정부와 기업의 정보화 그리고 산업전반의 혁신적인 변환 노력의 전략적 일환으로 CALS(Commerce At Light Speed)/EC(Electronic Commerce)가 상당한 관심을 끌고 있다.

CALS/EC의 출현은 컴퓨터가 한 개인 및 조직을 대상으로 대내적으로 이용되던 산업사회로부터 통신기술의 발달과 함께 전세계적인 사회 공동체가 참여하는 대외적 환경요소가 더욱 증가됨에 따라 21C 정보사회로 전환되는 시점에서 전개되고 있는 컴퓨터 기술이다.

CALS/EC 개념이 출현하기까지 컴퓨터의 이용환경은 수많은 변천을 거듭하였다. 이는 초창기의 단순한 전자적 자료처리개념의 EDPS(Electronic Data Processing System)가 개

* 대구미래대학 컴퓨터정보처리과 전임강사
** 대구미래대학 멀티미디어정보과학과 전임강사

인 및 조직의 생산성 향상을 위해 도입된 이래, 한 조직의 생산성 향상을 위한 통합정보화 개념의 CIM(Computer Integrated Manufacturing)/MIS(Management Information System), 그리고 오늘날 보다 확장된 대내외의 통합정보화 체제구현을 위한 CALS/EC로 변천되고 있다. 이것은 컴퓨터와 통신기술의 발달로 산업구조가 급격히 변화되고 있음을 시사하는 것이나, 현재의 산업구조는 이러한 변천과정의 중간적인 모든 이용형태를 포함하고 있다. 따라서 다양한 이용환경에서 표준화는 무엇보다도 어려우며 대단히 중요한 항목이다. 즉, 컴퓨터를 이용한 정보처리 환경이 하나의 부서 및 기업에 종속적인 내적 환경에서 근래에 통신기술의 발전 및 인터넷 등의 활용 증가에 따라서 개방형 EDI(electronic Data Interchange), 전자지불 등 대외적인 환경에 보다 깊게 연관되고 있다.

이러한 현상은 가치를 공유하려는 대외적인 주체들 사이에 일종의 표준화 과정을 폭넓게 요구하게 된다. 만일 표준화 절차가 미흡하다면 호환성의 부재로 상호연결이 어렵고, 중복투자 개발의 낭비가 있으며, 서비스의 질이 저하되는 등 수많은 문제점을 포함할 것이다. 특히 대외적인 환경을 만족시키기 위한 원격지간의 다양한 통신행위는 과거의 대내적인 환경에서 경험하지 못한 수많은 정보보호 위협요소들의 문제를 갖는다[1][2][3][4].

그러나 정보보호기술은 전세계적으로 자국의 이익 보호차원에서 수출금지 항목이거나 높은 기술료를 부담해야 한다. 더구나 세계적인 표준 및 수입된 기술이 우리의 힘으로 완전히 분해되어 그것의 활용에 대한 안전성이 검증되지 않으면 자국의 정보가 수출국의 의지에 따라 노출될 위험도 있다. 따라서 CALS/EC 환경의 성공적 도입을 위하여 각 외국의 표준화 활동을 광범위하게 조사하고, 동시에 국내의 표준화 대책을 마련할 필요가 있다. 특히, 정보보호기술은 외국의 자국기술 보호정책과 수출금지의 특별한 여건을 고려하여 우리 스스로 개발해야 하는 중요한 부분이다. 또한 국제 표준의 경우에도 정보보호 기술이 CALS/EC 메커니즘에 정합될 경우에는 다양한 제약사항이 첨가될 것이므로 시기 적절한 CALS/EC 정보보호기술 표준화에 관한 국내 대책을 마련할 필요가 있다[3][5].

본 연구의 목적은 국내외적 CALS/EC 구현과 관련한 각 응용분야별 정보보호 기술 및 표준화 동향에 대한 분석을 통하여 국내 여건에 적합한 전략적인 표준화 방안을 모색하고자 하는 것이다.

Ⅱ. CALS/EC 정보보호 위협요소분석

전자상거래상에서 정보보호 표준을 도출하기 위해서는 우선 CALS/EC 서비스에 어떠한

정보보호 위협요소가 있는지 다음과 같은 요소들을 살펴볼 필요가 있다. 첫째, CALS/EC 서비스는 컴퓨터 통신망을 이용하여 처리되므로 이미 널리 알려진 컴퓨터 통신에서 발생될 수 있는 기본적인 요소를 조사해야 한다. 둘째, CALS/EC 구현기술 중 하나인 EDI 서비스와 관련하여 정의된 위협요소를 분석한다. 셋째, EDI 및 EC와 다른 측면에서의 특별한 CALS와 관련된 위협요소를 분석한다. 넷째, EC의 특별한 기능으로 분류할 수 있는 전자지불 등과 관련된 위협요소들을 분석함으로써 향후 효과적인 대응전략 수립을 위한 토대를 마련해야한다.

1. 컴퓨터통신 정보보호 요소분석

CALS/EC 서비스는 컴퓨터와 네트워크를 이용하여 수행되는 광의의 컴퓨터 응용기술이다. 컴퓨터 시스템 또는 컴퓨터 네트워크에서의 공격유형은 정보 제공자로서의 컴퓨터 기능을 살펴봄으로써 그 특성을 가장 잘 알아볼 수 있다. 일반적으로 정보의 흐름은 파일이나 주기억장치의 한 부분과 같은 정보의 출처로부터 다른 파일이나 사용자와 같은 정보의 목적지로 전달되는 과정을 갖는다.

이와 같은 정상적인 정보의 흐름에 대한 네 가지 공격 유형이 존재한다. 첫째, 방해로 시스템 일부가 파괴되거나 사용할 수 없는 경우에 가용성에 대한 공격으로서, 예를 들면 하드웨어 일부의 파괴, 통신회선의 절단, 또는 파일 관리 시스템의 무력화되는 경우이며, 둘째 가로채기로 비 인가자의 불법적 접근에 의한 신뢰성에 대한 공격으로서 비인가자는 사람, 프로그램 또는 컴퓨터일 수 있으며, 네트워크상에서 데이터를 가로채기 위한 도청과 파일 또는 프로그램의 불법 복사 등을 예로 들 수 있으며, 셋째 불법 수정으로 비인가자의 불법접근뿐만 아니라 불법적 변경에 의한 무결성에 대한 공격으로 데이터 파일내의 값 변경, 프로그램의 다른 기능 수행을 위한 변조, 네트워크상에서 전송중인 메시지 내용의 수정 등을 말하며, 넷째 비인가자의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격으로 네트워크상에 위조된 메시지를 삽입하거나 파일에 레코드를 추가하는 경우이다[2][4][6][7].

이들의 공격형은 다시 소극적 공격과 적극적 공격으로 나눌 수 있다. 소극적 공격이란 전송정보에 대한 도청이나 감시를 말한다. 적의 목적은 전송중인 정보를 획득하는 것으로 메시지 내용 공개와 트래픽 분석 등 두 가지 유형의 공격으로 나눌 수 있다. 첫째, 메시지 내용 공개는 전화통화, 전자우편 메시지, 전송파일 등에는 기밀정보가 포함되어 있을 수 있으며 공격자가 이들 전송 내용을 탐지하지 못하도록 예방해야 하며, 둘째 트래픽 분석은 암호장치를 적소에 배치해도 공격자는 암호 메시지의 유형을 관찰할 수 있으며, 공격자는 통신자의 장소와 실체를 파악하고 메시지 교환횟수와 길이를 알아낼 수 있다. 따라서 이와 같은 정보는 통신의 성

격을 추측하는데 유용하게 이용될 수 있으며, 실제로 소극적 공격은 데이터를 변형하지 않기 때문에 탐지가 어렵지만 예방할 수 있다. 적극적 공격은 데이터 스트림의 불법수정이나 거짓 데이터 스트림의 생성을 수반하며, 신분위장, 재전송, 메시지 불법수정 그리고 서비스 부인의 4가지로 범주로 나뉜다. 첫째, 신분위장은 하나의 개체의 행세를 할 때 발생하며, 대개는 적극적 공격의 다른 유형 중 하나를 포함한다. 예를 들면, 인증순위를 알아내어 정당한 인증순서대로 진행된 후에 그 순서대로 재 전송하여 어떤 소수의 특권으로 인증된 개체가 추가 특권을 가진 개체로 행세를 함으로써 그 추가 특권을 획득하는 것이다. 둘째, 재전송은 하나의 데이터 단위를 수동적으로 획득하여 비 인가된 결과를 초래하기 위하여 다시 전송하는 일을 수반하며, 셋째, 메시지 불법 수정이란 단순히 적법한 메시지의 일부가 불법 수정되거나 메시지 전송의 지연, 순서 등을 변경시키는 것을 말하며, 마지막으로 서비스 부인이란 통신설비가 정상적으로 사용되거나 관리되지 못하게 방해하는 것을 말한다. 또 다른 형태의 서비스 부인은 네트워크를 무력화하는 것을 말하며, 또 다른 형태의 서비스 부인은 네트워크 전체가 와해되는 경우이다.

따라서 소극적 공격의 경우 발견은 어렵지만 예방 수단은 가능하나, 적극적 공격의 경우는 완전한 예방이 어렵다. 그 이유는 모든 통신설비와 통신경로를 항상 물리적으로 보호해야 하기 때문에 완전하게 예방하기보다는 공격을 발견하고 또 공격에 의한 와해나 지연 등으로부터 복구하는 것을 목표로 한다[5][6][7][8].

1.1 정보보호 서비스

① 기밀성

소극적인 공격으로부터 전송자료를 보호하는 것으로 가장 일반적인 서비스는 두 사용자간에 모든 전송자료를 일정기간 보호하는 것이다. 예를 들어, 두 시스템 사이에 가상회로가 개설되었다면 그 가상회로상에 전송된 모든 사용자 자료가 공개되지 않도록 보호하는 것으로 이는 단일 메시지내의 특정필드에 대한 보호역할을 한다. 기밀성은 트래픽 흐름분석에 대한 보호로서 전송자료의 출처와 목적지, 횟수, 길이, 통신선로상의 트랙픽 특성에 대하여 공격자가 알지 못하게 하는 기능도 한다[8].

② 인증

컴퓨터 네트워크의 사용에는 다양한 실체들을 확인할 필요가 있다. 이에 해당하는 실체에는 물리적 실체(예, 컴퓨터시스템), 논리적 실체(예, 통신계층의 각 실체 또는 응용프로그램) 그리고 사용자 자체이다. 인증이란 이러한 실체를 가장하여 컴퓨터 네트워크에 침입하는 경우를 대비하여 정확하게 실체를 가장하여 컴퓨터 네트워크에 침입하는 경우를 대비하여 정확히 실체를 확인하는 작업을 의미한다. 이러한 인증성을 보장하기 위한 메커니즘으로는 디지털 서명이

있다. 인증서비스는 통신이 신뢰성을 갖도록 보증하는 것이 매우 중하므로 인증서비스는 통신이 신뢰성을 갖도록 보증하는 것이 매우 중요하다.

이러한 안전한 통신환경을 유지하기 위해서는 원거리 신원확인을 함으로써 통신상대자가 적법한 상대자인가를 알아야 하고, 상대방에게도 자신이 적법한통신 상대자라는 것을 인식시켜 주어야 한다[8][9].

③ 메시지 인증

메시지가 송신 또는 전달 도중에 어떠한 변경이나 위조 없이 수신자에게 전달되었다는 것을 확인하는 절차로 크게 통신문 복원법과 인증자 조회법으로 대변할 수 있다.

통신문 복원법은 수신 측에서 복원된 통신문의 의미가 정당한 지를 인증하는 것으로 메시지 전체의 암호문에 의해서 인증자를 만드는 것으로 송신자가 통신문과 비밀키를 이용하여 암호화하게 되고, 수신자는 서명문을 복호화하여 복호화된 내용의 의미가 있는지의 여부를 인증한다. 만일 의미가 없는 내용이면 원래의 메시지와 다른 변경이나 위조가 발생하였음을 알 수 있다. 또한 부속 정보로 일련번호나 시간정보(time stamp)를 이용하여 안전성을 높일 수도 있으며, 비밀키 암호나 공개키 암호로도 실현될 수 있다.

인증자 조회법은 패리티 검사 부호와 원리적으로 유사하지만 패리티 비트에 해당되는 인증자를 해쉬함수와 비밀키를 이용하여 발생하는 점이 다르다. 따라서 송신자가 메시지 m에 비밀키와 단방향 해쉬함수 h를 이용하여 서명문인 인증자 h(m)를 발생하여 메시지 m과 함께 수신자에게 보낸다. 이때 수신자는 수신된 메시지 m과 자신의 비밀키 그리고 해쉬함수 h를 이용하여 새로운 인증자 h(m)을 만들어 수신된 송신자의 인증자와 조회해보고 만일 일치하면 송신자의 메시지는 변형없이 정확한 것임을 인증받게 된다. 인증자 조회법의 대표적 것으로 DES를 이용하는 MAC(Message Authentication Code)이 있으며 메시지 인증방식으로 가장 많이 사용되고 있다[8][9][10].

④ 사용자 인증

이 기술은 사용자의 정당성을 식별하는 기술로 키나 카드 등 본인만 가지고 있는 것을 식별하는 방법으로 패스워드, 비밀키 등 본인만이 알고 있는 정보를 이용하여 식별하는 방법으로 지문, 음성, 사인, 망막, DNA 정보 등 본인의 신체의 특징 정보를 이용하여 식별하는 방법이다. 본인만이 가지고 있는 정보나 본인만이 알고 있는 정보는 분실, 도난, 망각 등의 가능성이 있기 때문에 신체의 특징 정보를 이용하는 가장 안전한 방법으로 알려져 있다. 그러나 이를 직접 구현하여 사용하기에는 많은 양의 데이터베이스 관리 등 실상의 문제점이 많아 특수한 용도에 한하여 사용되고 있다. 사용자 인증 기술은 본인만이 갖고 있거나 알고 있는 정보를 이용하여 식별하는 방법은 암호를 이용할 경우 안전하고 실용적인 사용자 인증방식이 될 수 있다. 따라서 사용자 인증기술로 널리 알려져 있는 방식은 패스워드 이용방식, 일회용 패스워드(One

time password)방식, 시도응답방식(Challenge response)을 이용한 방식이 있다[10][11].

⑤ 무결성

무결성 유지는 인가된 사용자에 의해서만 파일 자료를 변경할 수 있도록 하여 비인가자 및 불법 사용자의 파일에 대한 기록, 삭제, 생성, 변경 등 접근으로부터 정보를 보호할 수 있어야 한다. 무결성 유지를 위한 메커니즘으로는 물리적 통제와 접근 제어를 들 수 있으며 또한 이미 변경되었거나 변경 위험이 있을 때 이를 탐지하여 복구할 수 있는 메커니즘도 필요하다. 기밀성 서비스와 같이 무결성 서비스는 메시지 스트림, 단일 메시지, 또는 메시지의 특정 필드에 적용될 수 있다. 앞에서 언급한 바와 같이 가장 유용하고 직접적인 접근 방법은 메시지 스트림 전체를 보호하는 것이다. 메시지 스트림을 대상으로 하는 연결형 무결성 서비스는 메시지가 원래 송신된 대로 즉, 복사, 추가, 수정, 순서 변경 또는 재전송 되지 않고 수신됐음을 확인하는 것이다. 자료에 대한 파괴 또한 이 무결성 서비스에 의하여 다루어진다. 따라서, 연결형 무결성 서비스는 메시지 스트림의 불법수정과 서비스 부인 모두를 강조한다. 한편, 비연결형 무결성 서비스는 어떤 환경에 상관없이 개인 메시지들만을 대상으로 하며 일반적으로 메시지 불법 변경으로부터 보호한다.

무결성 서비스에서 복구를 포함한 경우와 포함하지 않은 경우 차이가 있다. 무결성 서비스는 적극적 공격과 연관되기 때문에 예방보다는 발견에 더 관심을 두어야 한다. 무결성에 대한 침해가 발견되었을 경우 서비스는 단지 그 침해사항을 보고하며, 그 침해사항을 복구하기 위해서는 소프트웨어나 사람의 개입이 필요하다[9][10][11].

⑥ 부인 봉쇄

부인봉쇄란 송신자나 수신자가 전송 메시지를 부인하지 못하도록 하는 것이다. 따라서, 메시지가 송신됐을 때 수신자는 메시지가 실제로 송신자에 의해서 송신됐음을 확인할 수 있다. 반대로 메시지가 수신됐을 때 송신자는 그 메시지가 실제로 수신자에 의해서 수신됐음을 확인할 수 있다[11].

⑦ 가용성

시스템이나 시스템내의 자료는 허가된 사람에게는 효율적으로 사용할 수 있도록 하여야 한다. 즉 정보가 손상되지 않고 사용하고자 할 때는 항상 획득이 가능하도록 데이터의 백업, 중복성 유지, 물리적 위협요소로부터의 보호를 유지함으로써 이러한 가용성을 높일 수 있다. 그러나 시스템 사용을 완전히 배제하는 완벽한 보안성과 가용성은 상호 이율배반적인 면이 있으므로 컴퓨터 네트워크 보안의 균형을 이루도록 절충하는 것이 바람직하다. 다양한 형태의 공격에 의하여 가용성에 손실이나 감소를 초래할 수 있다. 어떤 공격은 인증이나 암호화와 같은 자동화된 대책에 의해서 처리될 수 있으나, 어떤 다른 공격은 분산시스템의 요소에 대한 가용성의 손실을 예방하거나 복구하기 위해 물리적 조치를 필요로 한다[10][11].

1.2 정보보호 메커니즘

① 접근제어

네트워크 보안에서 접근제어란 통신 링크를 통한 호스트 시스템과 응용간의 접근을 제한하고 제어할 수 있음을 의미한다. 이와 같은 제어를 달성하기 위하여 각 실체에 접근 권한이 주어지도록 접근을 얻으려는 각 실체는 우선 식별되어야 하고, 또한 인증과정을 거쳐야 한다. 접근제어 메커니즘은 접근제어 정보, 패스워드와 같은 인증정보, 자격·소유 그리고 부차적 표시, 보호레이블, 접근이 시도된 시간, 접근이 시도된 경로, 접근지속시간 등이 있다.

접근제어 메커니즘은 통신의 끝점이나 중간점에 적용이 가능하며, 발신이나 중간점에 적용된 접근제어는 송신자가 수신자와 통신하기 위해 인증되어야 하는지 혹은 요구된 통신자원을 사용하기 위해 인증되어야 하는지를 결정한기 위해 사용된다[12][13].

② 디지털 서명

디지털 서명 메커니즘은 데이터에 대한 서명과 서명된 데이터에 대한 검증절차이다. 서명은 서명자의 비밀정보인 비밀키를 사용하여 데이터 암호화나 점검 값을 생성하는 과정이며 검증은 서명자의 공개정보를 사용하여 정보를 보낸 사람이 누구인지를 아는 과정이다. 디지털 서명은 공개키 암호가 제공할 수 있는 하나의 특징으로, 수신자가 받는 메시지의 변조나 위조를 방지하며, 메시지의 송신자가 추후 부인할 수 없도록 하는 것으로, 메시지 인증과 사용자 인증을 동시에 수행하는 것이다. 비밀키 암호를 이용한 메시지 인증에서는 송신자와 수신자 사이의 분쟁 발생시 문제 해결이 곤란하지만, 디지털 서명에서는 제3자의 중재를 통하여 분쟁을 해결할 수 있어 전자상거래 등에 널리 활용될 수 있다[12][13].

③ 트래픽 패딩

트래픽 패딩은 트래픽 해석을 막는 다양한 레벨을 제공하도록 사용될 수 있으며, 트래픽 패딩이 비밀보장 서비스에 의해 보호된다면 효율적이다[12].

④ 경로제어

경로는 물리적으로 안전한 서브 네트워크, 릴레이 혹은 링크를 사용하기 위해서 유동적으로 혹은 미리 지정함으로써 선택할 수 있다. 단말 시스템은 지속적인 공격에 대해서 망 서비스 공급자에게 다른 경로를 경유해서 연결을 설립하도록 지시할 수 있다. 어떤 보호레벨을 가지는 데이터는 보호방침에 따라 서브 네트워크, 릴레이, 혹은 링크를 통해 전송되는 것이 금지 될 수 있으며, 접속 설정자나 비접속 데이터 단위 송신자는 특정한 부 네트워크, 릴레이, 그리고 링크를 피하도록 경로 절차를 규정해야 한다[12][13].

⑤ 공증

공증 메커니즘은 통신중인 데이터의 무결성, 출처(source),시간 및 목적지 같은 특성들을

보증하는 것이며 이러한 보증은 통신 실체들 간에 신뢰할 수 있는 제3자에 의해 이루어진다. 각 통신 실체는 공증 서비스를 제공하기 위해 디지털 서명을 사용할 수 있다[12].

⑥ 신뢰기능

신뢰기능은 다른 보호 메커니즘들의 영역을 확장하거나 효율성을 확립하는데 사용되며, 구현하기가 어려울 뿐 아니라 비용도 많이 든다. 이러한 문제들을 보호기능의 구현을 허용하는 구조를 선택함으로써 최소화할 수 있다. 보호가 적용된 계층상의 보호속성은 다른 방법에 의해서 제공되어야 한다[12].

⑦ 보호레이블

보호레이블은 자원의 민감성 정도를 나타내는 것으로, 데이터 전송시 적당한 보호레이블을 전송하는 것이 가끔 필요하다. 보호 레이블은 전송된 데이터와 연관된 데이터와 연관된 부가적인 데이터일 수 있고, 데이터를 암호화하는데 사용된 키를 나타낼 수 있으며, 출처나 경로와 같은 데이터 내용을 나타낼 수 있다. 또한 보호레이블은 관련된 데이터에 안전하게 결합되어져야 한다[13].

⑧ 사건감지

보호관련 사건감지는 보호위반 사건과 정상적인 접근사건 감지를 포함한다. 보호관련 사건들은 보호 메커니즘들을 포함하는 OSI의 실체들에 의해서 감지된다. 이러한 보호관련 사건의 예로는 보호위반, 발생수의 폭주(overflow) 등이 있다[13].

⑨ 보안감사

보안감사 추적은 보안감사를 첨가함으로써 보호가 깨진 곳을 찾고 조사하도록 하는 보호메커니즘을 제공한다. 보안감사는 시스템제어의 타당성을 검사하고, 확립된 정책과 동작절차를 준수하는 것을 확인하고, 손해 사정의 관점에서 지원하며, 제어, 정책과정들의 변화를 추적하기 위하여 시스템 기록들과 활동 등을 독립적으로 시험하고 재검토하며, 추적에서의 보안관련정보의 기록과 보안감사 추적으로부터의 정보의 보고와 분석을 요구한다. 일지나 기록은 보안메커니즘으로 고려되고 분석과 보고생성은 보안관리 기능으로 고려된다[13].

2. EDI 정보보호 요소 분석

CALS 체제는 국가경쟁력 향상을 위한 중요한 요소로서 표준화된 다양한 디지털 정보를 송수신 하는데 필수적이다. 현재 CALS만을 위한 하드웨어나 소프트웨어가 개발되지 못한 상태이므로 CALS 체제의 구축을 위해서는 새로운 것을 개발하기보다는 지금까지 개발되어 사용중인 하드웨어를 활용하여 구축될 필요가 있다. CALS 체제의 구축은 현재 전자적 문서 교

환인 EDI가 활용되고 있으며, 이러한 EDI를 확장하여 통합 데이터베이스와 결합시킴으로써 구축될 수 있을 것이다. 또한 CALS 정보보호도 현재 분석된 EDI 정보보호를 바탕으로 확장함으로써 CALS 정보보호가 분석될 수 있다[14].

2.1 EDI 정보보호 위협요소

EDI는 기업과 기업간에 거래문서를 컴퓨터 처리가 가능하도록 구조화된 형태로 통신망을 통해 상호 교환하는 고부가가치의 정보통신서비스이다. EDI는 구조화되고 표준화된 전자상거래 문서를 상호 교환함으로써 E-mail, FAX와는 달리 컴퓨터간 거래를 할 수 있고 기업간, 업종간, 산업간, 국가간 수평적인 정보유통이 가능하다. EDI문서는 상업적인 거래 문서로 정보보호 문제가 생길 수 있으며, EDI로 업무를 처리하기 위해서는 전자문서의 송수신시 정당한 권리를 갖고 있지 않은 제3자가 관련 데이터를 변조, 훼손 또는 첨가하는 것을 방지하고 거래당사자가 송수신 사실을 부인하지 못하게 하는 정보보호 대책이 필요하다.

수·발주, 계약서 등 EDI를 통하여 거래되는 문서는 각 기업의 이익과 직결되기 때문에 무역, 금융, 유통, 운송을 포함한 각 분야에서 EDI를 이용할 때 정보보호 문제가 해결되어야 한다. 그러므로 EDI를 위협하는 요소들이 분석되어야 하며 EDI 위협요소는 MHS 위협요소에 상거래상에 나타나는 몇 가지 위협요소가 부가된 것으로 볼 수 있다. 위협요소는 개별적으로 또는 둘 이상의 위협들이 복합적으로 일어날 수도 있으며 이러한 위협요소에 대한 대응책으로 정보보호 서비스를 제공하며 필요한 정보보호 메커니즘을 활용한다.

EDI에서 제공되는 정보보호 서비스는 MHS에서 지원하는 정보보호 서비스와 EDI에서 사용하기 위해 추가로 확정된 정보보호 서비스를 포함하며, EDI 정보보호 서비스는 발신처 인증 서비스, 안정한 접근 관리 서비스, 데이터 기밀성 서비스, 데이터 무결성 서비스, 부인봉쇄 서비스, 메시지 정보보호 레이블링 서비스, 정보보호 관련 서비스가 있다. EDI에서 확장된 정보보호 서비스로는 EDIM 책임인증 및 부인봉쇄 서비스가 제공된다. CALS에서는 EDI와 같은 메시지 교환시스템이 사용되고 있으며 EDI에서 제공되는 정보보호 서비스는 기본적으로 제공되어야 한다.

전자상거래에서 EDI시스템이 중요한 이유는 전자적으로 교환되는 문서들이 무역, 운송, 유통, 금융 등 각 분야에서 사용될 때 반드시 해결해야 할 보안문제 때문이다. 그 이유는 EDI에서 거래되는 모든 문서는 예를 들면 송장(Invoice)이나 입찰서 등과 같이 실제 각 기업이나 조직의 이익과 직결되는 중요한 서류들이기 때문이다.

EDI시스템은 MHS 환경을 기반으로 하는 시스템으로서 기존의 MHS 시스템이 가지고 있는 위협요소들에 EDI시스템에서만 발생할 수 있는 위협요소가 추가되었으며, EDI 시스템에서

만 발생하는 보안 위협요소는 다음과 같으며, 이러한 위협요소들은 고의적으로나 사고에 의해서 발생할 수 있으며, 능동적 또는 수동적일 수 있다. 또한 둘 이상의 보안 위협요소가 복합되어 발생할 수도 있으며, 다음과 같이 7가지로 요약할 수 있다[14][15][16][17].

① 위장(Masquerade)

어떤 실체를 다른 실체인 것처럼 위장하는 것으로서 비인가 된 MTS(Message Transfer System) 이용자가 MTS facility를 불법적으로 액세스하기 위하여 제3자가 정당한 UA (User Agent) 혹은 MS(Message Store)인 것처럼 위장하는 것과 비인가적 MTA (Message Transfer Agent)가 UA, MS, MTA에 대해서 불법적으로 정당한 MTA인 것처럼 위장하는 것이 있을 수 있으며 이는 MTS의 위장, 거짓 수신 확인, 메시지 발신의 거짓 주장, MTS 사용자에 대한 MTA 위장, 다른 MTS에 대한 MTA 위장 등과 같은 사항이 포함한다.

② 메시지 순번 변조(Modification Message Sequence)

메시지의 일부 혹은 전부를 지연전달 시키거나 고의적으로 메시지를 재발급 혹은 순번을 재배치하는 것으로서 이는 메시지 replay, 메시지 reordering, 메시지 preplay, 메시지 지연 등과 같은 사항을 포함하고 있다.

③ 정보 변조(Modification of Information)

수신자에게 전달되는 정보, 라우팅 정보 및 관리 정보를 손실되게 하거나 변조하는 것으로 이는 메시지 변조와 파괴, 라우팅 및 관리 데이터 파괴 등과 같은 사항을 포함하고 있다.

④ 서비스 거부(Denial of Service)

엔티티가 자신의 기능을 수행하지 못하거나 상대방으로 하여금 기능 수행을 방해하는 것으로서 액세스 거부, 통신거부, 메시지 수신 금지, 과잉 트래픽 조작 등이 있으며, 이는 통신부인, MTA 고장, MTS flooding 등과 같은 사항을 포함하고 있다.

⑤ 부인(Repudiation)

MTS 사용자 혹은 MTS 메시지 전송, 제출, 배달 등의 행위를 실제로 하고서도 하지 않았다고 부인하는 것으로 이는 발신부인, 제출부인, 배달부인 등과 같은 사항을 포함한다.

⑥ 정보 노출(Leakage of Information)

메시지 전송 감시, MHS내의 정보에 대한 비인가적 액세스, 혹은 위장 등에 의해서 비인가자에게 정보를 노출시키는 것으로서 기밀성 손실, 익명성 손실, 메시지 남용, 트래픽분석 등을 포함하고 있다.

⑦ 기타

이 밖에 정보보호 레이블 관련 위협은 Misrouting, 발신자의 불명확한 메시지 레이블 사용, MTS 사용자의 불명확한 context 사용, Incompatible labeling policy 등이 있다.

3. CALS 정보보호 요소분석

3.1 CALS 정보보호 위협요소

CALS는 DEI와 통합 데이터 베이스를 통하여 기업내, 기업간 디지털 정보가 교환 또는 공유되기 때문에 EDI의 확장된 개념으로 볼 수 있으며 정보교환과 공유시 다양한 위협요소가 존재할 수 있다. CALS에서 교환되는 정보는 매뉴얼, 설계도, 보고서, 계약서 및 수·발주서류 등이 포함되며, 통합 데이터베이스에 의해서 관리 및 공유된다. 따라서, CALS에서는 EDI의 단순한 메시지 교환에서 일어나는 위협과 통합 데이터베이스에 대한 위협이 공존하기 때문에 정보보호의 대상 및 위협요소가 확장된다.

CALS위협요소는 대부분 전송되는 메시지를 변조하는 경우, 사용자의 특권을 얻어 위장하는 경우이기 때문에 EDI와 CALS에서 전송간에 거의 동일하게 존재하나, CALS에서는 통합 데이터베이스로 인하여 이에 대한 위협요소도 존재한다. 통합 데이터베이스에 권한 없는 기업이 권한 있는 기업으로 위장해서 정보를 요청할 수 있으며, 요청된 정보가 통합 데이터베이스로부터 전송될 때 네트워크상에서 위조, 변조, 도청 등의 위협요소들이 존재한다. 또한 내부자에 의한 정보노출 및 자연적인 재앙, 시스템 장애 등이 발생될 수 있다.

이를 토대로 CALS 위협요소를 다음과 같이 자연적으로 발생되는 위협요소와 고의적으로 발생될 수 있는 위협요소로 분류하였다[16][17][18].

① 자연적인 위협요소

- 자연적 재앙 : 자연적인 현상으로 발생되는 위협들로서 화재, 홍수, 지진, 화산, 태풍, 폭풍우 등이 있다.
- 에러 및 손실 : 사용자의 에러 및 오조작으로 인하여 발생되는 위협들로서 환경제어손실, 데이터 수정, 오조작 등이 존재한다.
- 정보관리부실 : 관리자의 부주의로 발생되는 위협들로서 장비의 재배치 비적절한 유지보수 등이 있다.
- 네트워크 장애 : 네트워크 장애로부터 발생되는 위협들로 비밀채널, 트래픽 장애 등이 있다.
- 시스템 장애 : 정보 시스템의 장애로 발생되는 위협들로서 전원 고장, 케이블 절단, 정전기, 하드웨어 시스템 결점 활용, 키 관리 시스템 파괴 등이 존재한다.

② 고의적인 위협요소

- 내부의 적 : 내부자로부터 권한의 남용으로 인하여 발생되는 위협들로서 권한 오용, 의

도된 신뢰 활용, 특권 프로그램 오용 등이 있다.

- 산업첩보 행위 : 프로그램이나 제품에 삽입함으로써 필요한 정보를 얻는 위협들로서 트로이 목마, 트랩도어, 바이러스, 웜 등을 들 수 있다.
- 컴퓨터 해킹 : 대부분 시스템을 파괴할 목적으로 공격자들로부터 발생되는 위협들로서 보호 설정 오류활용, 스피핑과 위장, 작업 획득, 패스워드 추측, 불완전한 데모 활용, 프로세스 우회, 재생 공격, 암호해독, 전송 중 감시, 전송 중 수정 등이 있다.
- 위장 : 어떤 객체가 마치 다른 개체인 것처럼 위장하는 것으로서 비인가 된 이용자가 자원을 불법적으로 접근하기 위하여 제 3자가 정당한 사용자인 것처럼 위장한다.
- 메시지 순서 변조 : 메시지의 일부 혹은 전부를 지연 전달시키거나 고의로 메시지의 재발급 또는 순서를 재배치한다.
- 정보 변조 : 수신자에게 전달되는 정보, 라우팅 정보 및 관리 정보를 손실되게 하거나 변조하는 것이다.
- 서비스시 거부 : 객체가 자신의 기능을 수행하지 못하거나 상대방의 기능 수행을 방해하고 제공된 서비스를 거부하는 것이다.
- 부인 : 시스템 사용자가 메시지 전송, 제출, 배달 등의 행위를 실제로 하였음에도 불구하고 하지 않았다고 부인하는 것이다.
- 정보 누출 : 메시지 전송 감시, 시스템내의 정보에 대한 비인가적 접근, 또는 위장 등에 의해서 비인가자에게 정보를 노출시키는 것이다.
- 신분 레이블 변조 : 해당 자원에 접근을 제어하기 위한 신분 레이블에 관련된 요소들을 변조하는 것이다.

3.2 CALS 정보보호 서비스

안전한 CALS 구현을 위해서는 정보보호 서비스들이 요구된다. CALS에서의 정보보호 서비스는 앞절에서 정의한 다양한 정보보호 위협요소들로부터 정보를 안전하게 보호하기 위한 것이다. CALS 체제에서는 정보보호 서비스가 완전하게 제공되어야 하며 위협요소를 해결할 수 있어야 한다. CALS 체제에서 요구되는 서비스를 정의함으로써 CALS 구현시 신뢰성 있는 체제를 구축하기 위한 정보보호 모델을 제시하는 기준이 될 수 있다.

안전한 CALS 구현을 위해 제공되어야 하는 정보보호 서비스는 데이터 기밀성, 데이터 무결성, 인증, 부인봉쇄, 접근제어가 있다[18].

3.3 CALS 정보보호 메커니즘

CALS에서 요구되는 정보보호 서비스를 제공하기 위해서 다양한 정보보호 메커니즘이 요구된다.

① 암호화 알고리즘

암호화 알고리즘이란 평문을 암호문으로 바꾸어 주며, 암호문을 본래의 평문으로 복원하는 알고리즘이다. 대부분의 암호시스템은 암·복호화 과정에서 특정한 키를 사용하여 키를 알고 있는 자만이 암호문을 생성할 수 있고 특정 암호문을 평문으로 복호화할 수 있도록 하고 있다. 따라서 자료를 암호화시켜 보호하는 데는 알고리즘뿐만 아니라 키 관리를 어떻게 하느냐가 매우 중요하다[18].

② 디지털 서명

데이터의 서명과 서명된 데이터의 확인 절차를 거친다. 서명은 서명자의 개인적인 정보를 사용하고 확인 절차는 공개적인 절차 및 정보를 사용하지만 이러한 정보로부터 서명자의 개인적인 정보를 도출해 낼 수 없어야 한다. 디지털 서명은 서명자의 문서적 행위를 제3자에게 간접적으로 증명할 수 있는 수단으로 서명자의 비밀키를 이용하여 서명하고자 하는 메시지의 함수로써 서명하는 서명생성 과정과 서명자의 공개키를 이용하여 서명을 확인하는 서명확인 과정으로 구분된다. 즉, 공개키 암호시스템에서 서명자가 소유한 비밀키로 메시지를 암호화하려면 그 결과가 서명이 되며, 이 서명은 누구나 서명자의 공개키로 복호화하여 그 결과가 일정한 규칙을 만족하는 의미 있는 메시지인가를 확인할 수 있다. 이와 같은 서명의 확인과정에서 원래의 메시지가 복원되는 서명방법을 메시지 복원형 디지털 서명이라고 한다. 대표적인 방법에는 DSS(Digital Signature Standard)가 있다[18][19].

③ 해쉬 알고리즘

메시지의 무결성 서비스를 위하여 중요한 정보의 무결성 확인과 메시지 인증 코드의 구성, 디지털 서명의 효율성 증대 등의 목적으로 사용한다. 해쉬 함수는 임의 비트 스트링으로 출력하는 함수로 많은 양의 정보에 대한 인증을 제공하는 것이며, 그 정보로부터 짧은 해쉬 결과에 대한 인증을 제공하는 것이다. 생성된 해쉬값은 블록 점검코드 혹은 암호화 점검값과 같은 보충적인 정보일 수 있고 그 자체가 암호화 될 수 있다[20].

④ 인증 메커니즘

송신 객체에 의해 제공되고 수신 객체에 의해 인증되는 패스워드와 같은 인증 정보의 사용, 암호화 기법, 객체의 소유 및 특색의 사용 등이 이용된다. 인증 교환 기법의 선택은 사용되는 상황에 따라 시간 스탬핑 및 동기클록, 양 또는 3방향 인증, 디지털 서명 및 공증에 의한 부인봉쇄 서비스 등을 들 수 있다. 시스템화된 인증 메커니즘으로는 Kerberos와 SESAME

(Secure European System for Application in a Multivendor Environment)가 있으며 통합 데이터베이스에 접근하는 클라이언트 인증에 사용 가능하다[18][19].

⑤ 접근제어 메커니즘

객체의 접근을 원하는 사용자가 자신의 신원을 제시하고 인증 시스템에 대한 접근을 위한 신원 인증을 받은 후 확인된 이용자가 객체에 대한 접근 권한을 확인하는 과정을 접근제어라고 한다. 접근제어 메커니즘은 특정 객체의 인증된 신원, 객체에 대한 정보 혹은 객체의 능력으로 접근 권리를 결정하고 접근하는데 사용 가능하며, 통신매체의 양단 중 어느 한쪽에 적용되거나 중간지점에 적용될 수 있으며, 임의적 접근제어(DAC : Discretionary Access Control), 강제적 접근제어(MAC : Mandatory Access Control), 역할기반 접근제어 등으로 구분된다. 임의적 접근제어는 주체의 식별(identification)에 근거하여 객체에 대한 접근 요구를 통제하는 방법으로 한 주체가 다른 주체에게 자신이 갖고 있는 권한을 넘겨주는 것을 허용하는 것으로 가장 일반적인 모델로는 접근 행렬 모델이다. 강제적 접근제어는 객체에 포함된 정보의 기밀성과 주체에 부여된 보안인가에 근거하여 수학적 보안 모델에 의한 보안 정책을 적용함으로써 주체의 객체에 대한 접근을 강제로 통제하는 방법으로 일반적인 모델로는 BLP모델, Lattice모델 등이 있다[18][19][20].

⑥ 정보보호 레이블 메커니즘

데이터를 포함하는 자원은 레이블을 표시하기 위하여 그들과 연관된 정보보호 레이블을 가질 수 있다[19].

⑦ 보안 감사 메커니즘

사용자들의 행위들을 로그 파일에 기록함으로써 상대방과의 문제 발생 시 감사를 위한 자료로 이용한다[19].

⑧ 키관리 메커니즘

정보보호 메커니즘이 활용되기 위해서는 자신만이 간직한 키의 관리가 매우 중요하다. 특히 기밀성을 제공하는 암호 알고리즘의 경우는 키 관리기술이 기본적으로 사용되며, 송신자와 수신자 사이의 키의 교환 및 공유가 CALS의 정보보호를 위하여 제공된다[19].

⑨ 경로설정 제어 메커니즘

전송되는 경로를 동적으로 혹은 사전배치에 의하여 선택할 수도 있으며, 지속적인 조작 공격을 감지하는 경우에는 종단 시스템 네트워크 서비스 제공자로 하여금 다른 경로를 통하여 접속하도록 지시할 수 있다[20].

⑩ 공증 메커니즘

무결성, 발신지, 시간 및 목적지와 같은 두 개 이상의 객체들 사이에서 통신되는 데이터에 대한 성질은 공증 메커니즘에 의하여 보증될 수 있다. 보증은 통신 객체에 의해 신뢰될 수 있

고 실증될 수 있는 방법으로 요구되는 보증을 제공하는데 필요한 정보를 보유한 제3자 공증에 의하여 제공될 수 있다[20].

4. EC 정보보호 요소분석

4.1 EC 정보보호 위협요소

전자상거래를 실용적으로 하기 위한 핵심은 전자결제시스템이다. 그래서 전자결제시스템은 신용카드로부터 시작하여 e-cash와 같은 네트워크형 전자화폐로 발전하고 있다. 그리고 전자결제시스템의 핵심 기술은 보안기술이다. 즉, 전자화폐의 발행, 결제 등의 단계에서 개인의 프라이버시와 이중 사용 문제를 해결하기 위해서 공개키 암호화, 디지털 서명 그리고 내용은닉서명(Blind Signature) 등의 암호기술이 사용되고 있다. First Virtual, Cyber Cash 그리고 e-cash 등으로 대표되는 인터넷형 전자화폐와 이론적으로 연구되고 있는 전자화폐 방식 중 최근 가장 관심을 끌고 있는 것은 Brands의 전자화폐 방식이다. 전자화폐는 사용자가 은행에 구좌를 개설하여 전자화폐를 발행받는 발행단계와 상점에서 물건을 사고 전자화폐를 지불하는 지불단계 그리고 상점이 은행에 전자화폐를 제출하고 자신의 구좌에 돈을 넣는 결제단계로 이루어진다. 전자상거래는 전자메일과 웹으로 이용하여 거래되어질 수 있다. 웹의 SSL은 송신자 부인 봉쇄를 지원할 수 있지만 메시지 전송증명은 지원하지 못한다. 전자메일을 이용할 경우에는 송신자 부인봉쇄와 메시지 전송증명을 지원함으로써 이와 같은 문제점을 막을 수 있다[21].

① 시스템 공격

일반적인 컴퓨터 시스템 특히 네트워크에 연결된 컴퓨터는 외부의 특정인이 이 시스템을 침입하여 부당하게 컴퓨터 시스템을 사용하거나, 정보를 유출하거나, 정보를 파괴할 위협이 있다. 일반적으로 이런 위협을 방지하기 위해 방화벽 같은 시스템을 사용하기도 한다. 그러나 전자상거래는 불특정 다수인의 접근을 허용하는 응용시스템으로서 방화벽을 사용하는데 있어서 제약을 받을 수도 있다 특히 시스템을 불법적으로 사용하는 통계를 보면 외부에서의 침입보다는 내부사용자의 불법적 사용이 더 많기 때문에 적절한 시스템의 운영지침과 재무사용자에 대한 보안대책이 중요한 요소가 된다[21][22].

② 데이터 공격

전자상거래에 있어서 데이터의 공격은 두 가지로 구분해 볼 수 있다. 하나는 시스템내에 저장된 데이터, 또 하나는 네트워크상에 흘러 다니는 데이터에 대한 공격이 있을 수 있다. 시스템에 저장된 데이터의 경우는 앞의 시스템 공격에서 언급되었고, 특히 데이터를 시스템에 저장할 때도 암호화를 해서 저장하는 것이 필요하다. 네트워크상에 흘러 다니는 데이터에 대한 공

격을 막기 위해 기밀성, 자료의 무결성 등에 대한 보증이 필요하게 된다[21][22].

③ Business 공격

앞에서 언급한 두 가지 공격은 모두 일반적인 컴퓨터 시스템의 보안침해와 동일하다. 그러나 전자상거래에 있어서는 상거래라는 특징 때문에 발생하는 제3의 공격이 있을 수 있다. 이것을 통칭해 비즈니스 공격이라 부른다. 상거래에만 일어날 수 있는 사기가 전자적 상거래에도 일어날 가능성이 있다. 이런 요소들은 전자적으로 막기 위한 보안 고려사항들이 추가적으로 필요하게 된다.

암호화 혹은 시스템으로만 모든 것을 다 막을 수는 없기 때문에 제도적인 장치, 법적인 보장, 보험 등의 전자적 시스템외적인 보완도 이루어져야 한다. 이런 취지에서 지난 1996년 6월에 UN의 국제상거래법위원회(UNCITRAL, United Nations Commission on International Trade Law)는 "전자상거래모델법(Model Law on Electronic Commerce)" 이라는 모델법을 통과시켜 공표했다[21][22].

④ 인터넷뱅킹 시스템 위협요소

인터넷뱅킹 시스템 위협요소로는 클라이언트 보안에서의 위협요소로 Virus, Trojan Horse 등이 있으며, 거래처리 보안에서의 위협요소로 Weak encryption, Server spoof 등이 있으며, 서버보안에서의 위협요소로 Unix/NT security holes, Improper administration 등이 있으며, 어플리케이션 보안에서의 위협요소로 Poor programming, Weak authentication 등이 있으며, 네부적인 보안에서의 위협요소로 Virus & Trojan Horse, Unix/NT security holes, Improper administration 등으로 구분할 수 있다[21][22].

4.2 EC 정보보호 서비스

4.2.1 전자지불 시스템에서의 정보보호 서비스

① 정보의 보호

전자지불시스템에 있어서 가장 중요한 요소는 바로 암호화기법이다. 인터넷은 안전하지 못한 네트웍으로 누구나 마음만 먹으면 네트워크상에서 주고받는 다른 사람의 데이터를 볼 수가 있기 때문에 자료암호화는 필수적인 요소이다. 네트워크상의 자료 암호화는 주로 공개키 암호화기법(Public Key Encryption Method)을 사용한다. 두 개의 키로 이루어지는 이 암호화기법을 통해 네트워크상에서 자료를 원하는 사람에게만 해독이 가능하게 암호화해서 전달하는 것이 가능해졌다. 이 기술은 현재 미국의 RSA(20)가 특허를 보유하고 있으나, 미국은 암호화기술을 무기로 간주하여 일정수주 이상의 암호화 장비/소프트웨어는 수출이 금지되어 있기 때문에 미국 이외의 국가에서는 RSA의 암호화기술을 도입할 수 없게 되어 있다. 이 때문에 미

국이외의 국가에서는 넷스케이프 브라우저와 넷사이트서버간에 암호화(SSL)통신을 한다고 하더라도 암호화키가 40bit 이하이기 때문에 사실상 암호화되었다고 볼 수 없어 안심할 수 없는 형편이다. 미국 이외의 국가에서는 이런 공개키 암호화소프트웨어를 판매하는 곳이 몇몇 눈에 띄긴 하지만 활발하지 않다. 공개키 암호화소프트웨어로 미국의 특허에 침해받지 않는 공개용 소프트웨어가 존재하지만 상당히 복잡한 것으로 알려져 있다[23].

② 전자서명(Digital signature)

컴퓨터의 디지털정보는 동일한 내용으로 복제가 가능하기 때문에 위조, 복제, 부인(否認)등이 용이하다. 이런 것들을 방지하기 위해 암호화기법과 더불어 디지털서명 등과 같은 추가적인 기술들이 개발되었다. 전자지불시스템에서 사용되는 전자서명은 특별한 방식으로 만들어진 디지털 정보인데, 이는 두 가지 기능을 한다. 하나는 메시지 인증기능과 사용자 인증기능을 갖는다. 메시지 인증기능은 비록 정보가 암호화되어 있다하더라도 이 내용이 처음에 만들어진 내용과 변경이 없다는 것을 증명하는 기능이고, 사용자 인증은 이 메시지를 보내 사람이 정말 내가 기대한 사람인지를 증명하는 기능이다. 사용자 인증을 수신하는 측에서도 유용하지만 메시지를 보낸 사람도 그 메시지를 자신이 보낸 것이 아니라고 부인하지 못하게 하는 효용이 있다[23].

③ 블라인드 전자서명(Blind Signature)

전자현금시스템에서는 사용자가 전자현금을 전자은행 혹은 전자지불회사로부터 인출할 때 일련 번호를 사용하는데 이때 은행은 사용자의 현금에 대한 정보를 획득하게 되고 사용자가 이를 사용했을 경우 은행은 사용자의 현금사용상황을 역추적 할 수 있는 정보가 된다. 이는 실세계의 현금이 갖는 익명성을 훼손함으로써 사용자의 개인정보를 침해한다. 이를 방지하기 위해 디지캐쉬사의 David Chaum이 고안한 서명기법으로서 은행은 사용자가 어떤 번호의 전자현금을 인출했는지를 알 수 없도록 하는 방식이다. 기본적인 아이디어는 사용자가 은행에 인출할 현금의 일련 번호를 제공할 때 불 특정한 숫자와 이 번호를 곱해서 은행으로 보내며 다시 이 번호를 전자현금화해서 사용자에게 넘겨주면 사용자는 이 번호를 곱한 숫자로 다시 나누어 원래의 번호로 환원해 사용하는 방식이다. 이렇게 하면 은행은 사용자의 원래의 현금번호가 무엇인지 알 수 없어 개인정보의 보호와 익명성이 보장되는 것이다[26].

④ 전자현금의 이중사용(Double Spending)

전자현금은 결국 디지털 데이터이다. 이는 동일하게 복사할 수 있기 때문에 사용자가 이를 복사해 현금을 두 번 이상 사용하는 것을 막아야 한다. 이에 대한 대안으로서 가장 손쉬운 방식은 현금을 받은 편에서 항상 은행에 이 현금이 두 번 사용된 것이 아닌지 물어보고 은행은 발행된 모든 전자현금의 사용 여부를 확인할 수 있는 데이터베이스를 유지해야 하는 어려움이 있다. 최근에는 은행에서 전자현금을 만들 때 특별한 방식으로 만듦으로써 이 현금을 받은 측이 은행에 사용 여부/복제 여부를 온라인으로 문의하지 않고 다만 수학적 방식으로 이의 복제

여부를 확인하는 방식이 계속 제안되고 있다[27].

4.2.2 전자 신용카드 거래시스템의 정보보호 서비스

① 상호 운용성

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

② 수용성(acceptability)

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

③ 호환성

인터넷상에서 사용되는 다양한 컴퓨터 플랫폼에서 호환성을 가지며 또한 이식성 및 확장성을 가질 수 있도록 표준화된 소프트웨어 개발이 필요하다.

4.2.3 전자화폐를 위한 정보보호 요구조건

① 독립성(Independence)

전자화폐는 주어진 컴퓨터 시스템 또는 장소와 무관해야 한다.

② 이중 사용(Double spending)과 위조방지

전자화폐를 재사용하거나 위조하는 것이 방지돼야 한다. 일반 지폐에 있어서 위조가 있으나 전자화폐에서는 이중 사용이 있다. 지폐에서의 위조는 은행 또는 정당한 발행기관의 허가 없이 돈을 만들거나 기존의 돈으로부터 새로운 돈을 만드는 행위를 말하지만, 전자화폐는 전자정보로 이루어져 쉽게 복사가 가능하다. 1회사용 후 다른 곳에 동일한 전자화폐를 사용할 수 있다. 전자화폐에 대한 이중 사용 방지는 사용된 전자화폐의 정보로부터 컴퓨터가 동일한 전자화폐를 조사하여 이중 사용자의 계좌번호와 사용자의 신분을 알아내는 방식을 주로 취하고 있다. 온라인인 경우 이중사용의 방지가 용이하나 오프라인인 경우 전자화폐 사용 전 거래중지가 곤란하기에 추후 부정 사용자 방지대책을 세워야 한다[26].

③ 익명성(Anonymity-Privacy/Untraceability) 보장

사용자에 대한 정보나 사용내역 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 전자화폐시스템의 효율을 떨어뜨릴 수 있기에 완전한

익명성의 구현은 신중이 고려되어야 한다[27].

④ 이동성(Transferability)

전자수표는 한 사람으로부터 다른 상대방에게로 쉽게 이동될 수 있어야 하며, 이 돈을 소유한 사람이 사용한 증거를 남기지 않고 발생시켜야 한다.

⑤ 분할성(Divisiability)

전자수표는 액면 금액을 개별적으로 이용 가능해야 한다. 예를 들어, 25 디지털 페니는 4등분의 디지털을 산출할 수 있어야 하고 4개의 4등분된 디지털은 1달러와 같아야 한다.

⑥ 안전한 기억장소(Secure Storage)

전자수표는 고객의 하드드라이브 또는 PCMCIA 카드와 같은 스마트 카드에 안전하게 저장되는 방법으로 이용 가능해야 한다. 더욱이, 인터넷상에서 다양한 상대방 유형간에 전자수표를 전송할 수 있어야 한다[27].

4.3 EC 정보보호 메커니즘

4.3.1 S-HTTP(Secure-HTTP)

S-HTTP는 EIT(Enterprise Integration Technologies)에서 제안한 HTTP의 Security 확장판이다. 프로토콜은 HTTP세션으로 주고받는 자료를 암호화, 전자서명 등을 지원하는 메커니즘이며, 현재 1.1버전의 draft가 http://www.commerce.net/information/standards/drafts/shttp.tst에 나와 있다. S-HTTP는 HTTP를 캡슐화하면서도 HTTP와 같은 메시지 기반 프로토콜이며, HTTP처럼 요청과 응답 구조를 그대로 이용하고 있다[18][26][27].

(1) S-HTTP 시스템 디자인 목표

① Enable Spontaneous Commercial Transactions
② Negotiation of Algorithms, Modes & Parameters
③ Layer separation (Don't "Fix" HTT)
④ Mechanism, not Policy, Trust Model Independence, Where do Certificates Come From?, What Do Certificates Mean?
⑤ Interoperability, With Existing Clients & Serves (w/o Security), With Implementations of Varying Capabilities

(2) 암호화메커니즘

① Encapsulation Format : PKCS-7, PEM or pGP

② Signature Algorithm : RSA or DSA

③ Key Exchange Algorithm : RSA, In-band, "Outband", D-H, Kerberos

④ Message Digest Algorithm : MD2, MD5 or SHA

⑤ Encryption Algorithm : DES, DES-EDE2/EDE2, DESX, IDEA, RC2, RC4

⑥ Protection Mode : Signature, Encryption, Keyed MAC

⑦ Public Key Certificate Format : X.509 or PKCS-6

(3) S-HTTP 개관

① 새로이 도입된 Anchor, Method

새로운 프로토콜 지시어로 "shttp"를 사용한다. 즉 S-HTTP로 통신을 하는 Anchor의 URL은 shttp://../ 형태로 새로이 제안되었다. 또한 요청(request) 포맷은 "Secure url Secure-HTTP/1.1" 형태로서 새로운 Method "Secure"를 새로이 정의해서 사용한다.

② 동작원리

S-HTTP는 HTTP처럼 Request-Response 구조를 가지고 있다. 다만 HTTP와는 다른 S-HTTP용 헤더정보를 통해 암호화방식에 대한 파라미터들을 주고받으면서, 서로 어떤 암호화방식으로 어느 정도 암호화해서 주고받을 것인가를 사전 조율한다.

③ 전송되는 문서의 암호화상태

- Unprotected : 암호화하지 않은 문서
- Signed : 전자서명이 된 문서
- Encrypted : 암호화가 된 문서
- Signed and Encrypted : 암호화하고 전자서명을 한 문서

(4) S-HTTP 구현사례

① NCSA

1994년 2월부터 10월에 구현을 완료했으며, 구현 범위는 서버 Unixtltmxpa에만 구현했고 브라우저는 모든 플랫폼에서 다 구현이 되었다. 이는 CommerceNet 컨소시움에서 의뢰해 개발된 것으로 해당 컨소시움 멤버에게 제공되었다.

② Terisa Syatems

상업용으로 테리사(terisa)시스템에서 구현해서 현재 개발툴킷으로 판매하고 있다. SecureWeb Toolkit(http://www.terisa.com/prod/index.html)이라는 이름의 제품을 판매하고 있다. 이 제품의 특징은 S-HTTP와 SSL을 모두 구현해두어서 한 툴킷으로 두 프로토콜응용 제품을 개발할 수 있다는 장점이 있다.

③ Open Market, Inc

Open Market사는 Secure WebServer(http://www. open market.com/products/servers/secure.htm)라는 이름으로 서버측의 S-HTTP구현 제품을 판매하고 있다.

4.3.2 WWW 보안

통신망을 이용한 전자상거래는 대부분 웹(WWW)을 기반으로 이루어진다. 웹은 하이퍼텍스트를 기반으로 뛰어난 사용자 인터페이스를 제공하기 때문에 널리 산재한 인터넷의 자원들을 효율적으로 검색할 수 있도록 해주고 상업 도메인에서는 웹이 제공하는 멀티미디어 기능을 활용하여 자사의 상품을 효과적으로 표현하여 사용자에게 실생활의 쇼핑몰과 유사한 효과를 제공한다. 이와 같은 웹을 전자상거래에 활용하기 위해서는 상거래시 전송되는 민감한 정보에 대한 안전성을 확보해야 한다[23][26][27][28].

(1) 웹의 보안상의 문제점

① 웹 구조상의 문제점

웹은 기본적으로 암호화 기능을 포함하고 있지 않으며, 프로토콜의 구조상 메시지를 암호화하기 어렵다. 특히 응용계층에서 구현되어 있는 웹은 기본적으로 IP spoofing에 대한 대책이 없으며 사용자 인증을 위한 패스워드마저도 단순한 스크램블 기법만으로 전달하도록 한다. 웹은 구조상으로 볼 때 정보 암호화, 접근제어, 디지털 서명 기법을 제공하고 있지 않으며, 인증기법만이 제공되나 그 기능이 매우 미약하다. 따라서 웹을 그대로 이용할 경우 중요한 문서의 유통 및 전자 상거래에는 부적합하다.

② 웹 브라우저의 문제점

웹 브라우저는 인터넷상에서 가장 크고 정교한 프로그램이라고 할 수 있으며, 하이퍼텍스트를 근간으로 구성되어 매우 복잡한 구조를 갖는다. 특히 브라우저는 HTTP 프로토콜뿐만이 아닌 다양한 프로토콜 및 형식을 지원하도록 하는 다기능 프로그램이다. 따라서 복잡한 프로그래밍에서 야기되는 보안 홀(Security Hole)이 있을 수 있으며, 이것은 침입자에게 악용될 여지가 많다. 특히 최근에는 브라우저가 다른 외부 응용 프로그램과 연결되어 실행되므로 여기서 비롯되는 많은 문제들은 정보의 보안에 있어서 심각한 위험을 가져온다. 일종의 플러그-인 기법이나 MIME helper 기능을 통하여 제공되는 외부 응용프로그램과의 연결은 다양한 형식의 정보를 처리할 수 있다는 장점을 제공하는 반면, 침입자에 의해서 악용될 우려가 있는 것이다.

(2) 현재 개발된 웹 보안기술

웹 보안기술은 웹 서버들이 기본적으로 제공하는 보안기능 외에, 보안 메커니즘이 제공되는

계층에 따라 응용계층에서의 보안과 네트워크 계층에서의 보안으로 나뉜다.

① 기본적인 웹 보안기능

■ 기본 인증(Basic Authentication): 사용자 인증이라고 불리는 이 메커니즘은 HTTP의 한 부분으로 초기부터 제공되었으며, 사용자에게 익숙한 사용자/패스워드 형태로 비교적 약한 인증기능을 제공한다. 기본 인증은 단순한 반면 관리가 어렵고 패스워드가 평문형태로 전달되므로 불안전하다.

■ IP 필터링(Filtering): 대부분의 웹 서버에서 제공되며, 기본 인증과 혼용될 수 있으며, 관리가 쉬운 반면, IP spoofing에 대한 대책이 없다.

② 응용 계층에서의 웹 보안

■ NCSA의 Mosaic/http의 PGP/PEM 인증 및 암호화: NCSA의 XMosaic과 httpd에 메시지 암호화와 서명을 처리하는 외부 프로그램을 실행할 수 있도록 기능을 추가한 예이다. 즉, PGP(Pretty Good Privacy)나 PEM(Privacy Enhanced Mail) 같은 독립적인 암호화 응용 프로그램과 연결하여 인증 및 암호화를 제공한다.

■ EIT의 Secure-HTTP: EIT(Enterprise Integration Technologies)에서 개발된 S-HTTP는 기존 HTTP 프로토콜에 보안 기능을 추가한 확장 버전이다. S-TTP는 DES, RC2, RC4, IDEA 등의 관용 암호화 방식, 그리고 MD2, MD5, SHS 등의 해쉬 알고리즘과 같은 다양한 암호화 알고리즘을 지원하며 앞서 설명한 NCSA의 방법과 유사하다.

■ Message Digest Authentication: 메시지 다이제스트 인증은 기본 인증을 간단히 대치하기 위한 것으로 패스워드가 평문의 형태로 전달되지 않도록 성능을 개선하였다. 즉, 일방향 해쉬 함수를 이용하여 패스워드를 암호화하여 보낸다.

■ Kerberized Mosaic/httpd: 커버로스(Kerberos)는 이미 네트워크 보안을 위해서 다양하게 적용되고 있는 프로그램이다. 특히 안전한 제3자의 개념을 이용하여 비교적 안전한 보안 시스템을 구축하도록 하고 있으나 넓은 범위를 갖는 영역에서 적용하기 어렵다는 단점이 있다.

③ 네트워크 계층에서의 웹 보안

■ Netscape's Secure Socket Layer(SSL): 웹의 보안을 개선하기 위해서 가장 최근에 시도되고 있는 방법이 바로 넷스케이프사의 SSL이며 이것은 인터넷 전반에 걸쳐 다양한 응용에서도 시도되고 있다. 주 아이디어는 웹 프로그램이 상주하는 응용 계층에서 메시지를 암호화하여 불안전한 채널로 전송하는 대신에, 응용 계층은 안전한 채널을 설정

하도록 하는 특수한 소켓 루틴만을 이용하고 어떠한 데이터라도 안전한 채널을 통해서 전송하도록 한다.

4.3.3 JAVA 보안기술

사용자에게 정적인 환경을 제공해 주는 HTML을 보강하고자 Sun Microsystems에서 발표한 JAVA는 바이트 코드(byte code) 형태로 응용프로그램을 전송하여 보다 동적인 웹 사용자 환경을 제공하는 기술이다. JAVA는 현재 개발자들을 위하여 JDK(JAVA Development Kit), 즉 개발자 라이브러리를 제공하고 있으며 1997년 4월에 발표된 JDK 1.1.1은 JAVA Security API와 JAVA Commerce API를 포함하고 있다[25][26][27] [28].

4.3.4 SSL(Secured Socket Layer)

SSL은 테리사(Terrisa)가 개발해 Netscape사가 Netscape와 NetSite의 암호화 중심 프로토콜이다. SSL은 서버와 클라이언트간에 인증(Certification)으로 RSA방식과 X.509를 사용하고 실제 암호화된 정보는 새로운 암호화 소켓채널을 통해 전송하는 방식이다. 특히 SSL은 네트워크 레이어의 암호화 방식이기 때문에 HTTP뿐만 아니라 NNTP, FTP 등에도 사용할 수 있는 장점이 있다.

4.3.5 SEA(Security Extension Architecture)

SEA는 W3C에서 최근에 만들고 있는 WWW Security 프로토콜로 WWW보안 프로토콜들이 있음에도 불구하고 W3C에서는 SSL/S-HTTP 두 프로토콜의 약점이 있다고 판단하여 HTTP 프로토콜과 더 밀접하게 관계를 가지는 새로운 보안 프로토콜을 제안했으며, SSL은 Transport층의 보안프로토콜이고 S-HTTP는 HTTP와는 비슷한 구조지만 별도의 새로운 프로토콜이어서 기존의 HTTP와의 호환성의 문제 등을 W3C에서는 문제시하고 있다. 또한 SEA는 S-HTTP의 기능을 수용하면서 구현은 W3C에서 최근 제안한 PEP을 이용하는 형태이다.

SEA를 이해하려면 PEP(Protocol Extension Protocol)의 구조를 이해해야 하며, PEP은 HTTP 프로토콜을 사용자 레벨에서 정의해서 확장할 수 있는 "프로토콜 확장 플랫폼" 프로토콜이며, 또 SEA는 이 PEP를 이용해 첫 번째 구현으로 SEA구현을 시도하고 있다.

PEP에 대한 정보는 http://www.w3.org/pub/WWW/TR/WD-http-pep.html에 있고, SEA에 대한 정보는 http://www.w3.org/pub/WWW/TR/WD-http-sea에 있다.

4.3.6 Secure Web

OSF DCE(Distributed Computing Environment)는 분산 컴퓨팅 환경에 대한 산업표준으로 보안 서비스를 제공하며 거의 대부분의 컴퓨팅 플랫폼에서 동작하며, 하드웨어 및 소프트웨어 환경에서 분산 응용을 제공하기 위해 설계된 것이다. 주요 소프트웨어 구성요소는 다중 프로토콜 서버(Multi-protocol server), SLP(Secure Local Proxy), SDG(Security Domain Gateway)이다.

① 다중 프로토콜 서버(Multi-protocol server)

다중 프로토콜 서버는 표준 http-over TCP와 Secure Web을 지원하는 고성능 확장 가능한 Web 서버이다. 이 서버는 단일 시스템이나 기존의 상용 Web 서버들과 함께 동작하도록 설계되었다.

② SLP(Secure Local Proxy)

표준사용 Browser들을 사용하여 Secure Web을 접근할수 있도록 하며, 현재 UNIX, Microsoft, Windows NT, 95, Apple Macintosh 등을 위한 버전들이 개발되었다.

③ SDG(Security Domain Gateway)

Secure Web에 다른 보안 프로토콜들을 통합시키는 역할을 하며, SSL을 사용하는 Browser를 위하여 Secure Web에 대한 안전한 접근을 제공한다.

DCE Secure Web에서 제공하는 보안 서비스는 데이터 무결성(Data Integrity), 상호인증(Mutual Authentication), 그리고 프라이버시다. 이러한 Secure Web에서는 서버 및 Client에서 인증 서비스가 제공되며, 접근통제, 프라이버시, 무결성, 감사 서비스가 제공되나 반면에 SSL에서는 Client에서의 인증 서비스가 미비하고 접근통제 및 감사 서비스가 제공되지 않는다.

4.3.7 S/MIME

S/MIME은 인터넷의 멀티미디어 전자우편 프로토콜인 MIME기능에 보안기능을 추가한 프로토콜로 아래의 세 가지 형태의 보안 기능을 지원한다.

- 전자서명(Signed)
- 데이터 암호화(Enveloped)
- 전자서명과 데이터 암호화(Signed and Enveloped)

S/MIME의 입력 데이터는 MIME, 메시지로서 MIME 메시지 전체에 대하여 전자서명 및 암호화 처리를 한다. 따라서 인터넷으로부터 수신된 S/MIME 메시지 처리 결과는 MIME 메시지가 된다. 가장 강력한 보안 기능을 제공하는 형식으로 전자서명과 데이터의 암호화는 전자서명과 암호화에 필요한 모든 데이터를 동시에 필요로 한다. 전자서명 방식에서 계산된

Message Digest는 송신자의 비밀키에 의해 암호화되고 그 결과는 다시 메시지 암호화에 사용된 대칭형 키로서 다시 암호화된다.

4.3.8 SET(Secure Electronic Transaction)

SET은 안전한 전자 트랜잭션 프로토콜의 명세로서 VISA사와 Mastercard사가 공동으로 제안하고 GTE, IBM, Microsoft, Netscape, SAIC, Terisa 그리고 Verisign사가 지원하기로 한 전자신용카드 거래 프로토콜이다. SET 명세는 1997년 5월에 버전 1.0이 발표되었으며, 1997년 중반부터 SET 프로토콜을 따르는 응용프로그램이 개발되고 있다. SET 프로토콜의 목적은 정보의 기밀성 제공, 지불정보의 무결성 확보, 상인과 고객 상호간의 인증에 있으며, 그 구성요소로서는 카드소지자, 상인, 지불게이트웨이, 인증기관 등이며, SET의 기본적인 프로토콜은 고객 등록 프로토콜, 상점등록 프로토콜, 구매 요구 프로토콜, 지불허가 프로토콜, 지불 capture 프로토콜 등이 있으며, 정보보호 요소 기술로는 암호화 알고리즘, 전자서명 및 해쉬함수, 전자인증서 등이 있다.

Ⅲ. 결 론

본 연구에서는 현재 전세계적으로 깊은 관심을 갖고있는 CALS/EC 구현과 관련하여 국내외의 추진현황과, 기반기술 및 각종 표준화 동향을 분석하였으며, CALS/EC 서비스의 안전성 위협요소에 대응하기 위하여 국내여건을 고려한 CALS/EC 정보보호기술 표준화 방향을 모색하는 것이 목적이다.

연구추진 방향은 CALS/EC의 개념적 정의, 국내외 추진동향 조사, 정보보호 위협요소 및 일반 정보보호 기술 표준조사 등이며, 위협요소에 대응할 수 있는 정보보호 서비스별로 기존 보안 표준의 이용방안 연구 등을 하였다.

따라서 본 연구 이후에는 이상에서 조사 분석된 결과를 토대로 CALS/EC 서비스의 궁극적인 실현을 위하여 필요한 정보보호 표준화 방향을 모색하고자 한다.

참 고 문 헌

1. 김철환 · 김규수, "21세기 정보화 산업혁명 CALS," 도서출판 문원, 1995, pp.13~18
2. 김규수 · 김철환외 3인 "산업정보화와 CALS," 한국 CALS/EC 기술협회 세미나, 1996, 6.
3. 김철환, "국방 CALS 구현사례," 한국정보처리학회지, Vol.4, No.1, 1997, 1.
4. 정기원, "국내기업의 CALS관련 정보화실태 및 SI업체 동향 조사," 한국 CALS/EC학회, 1993, 7.
5. 신장균 · 나영민 · 이승희, "CALS 구현을 위한 정보기술," 정보과학회지, 제13권 11호, 1995, 11.
6. 이임영 · 이재광 · 소우영 · 최용락, "통신망 정보보호," 도서출판 그린, 1996, 2.
7. 김중인 · 김석우, "CALS의 단계별 구현을 위한 보안기술," 정보보호와 암호에 관한 학술대회 자료집, 1996.
8. 이임영, "인터넷 전자상거래 보안," 제3회 한국전산망 보안기술 워크숍 특강자료집, 1996.
9. 김중인, "CALS 보안," 제3회 전산망 보안기술 워크숍 특강자료집, 1997, 5.
10. 임채훈, "인터넷 인증 및 공개키 기반구조," KRNET '97 발표자료집 II, 1997, 7.
11. 임신영 · 임창순 · 변옥환, "전자상거래 보안 시스템 및 암호화 기술의 적용," 제8회 정보보호와 암호에 관한 학술대회 논문집, 1996.
12. To. Carty, "GTE, Security Electronic Commerce, Certificate Management Systems," 9Th CITSS '97, 12-16 May, 1997.
13. Fred Cohen, "Large Information System Attack Methods : A Preliminary Classification Scheme," *Computer & Security*, Vol.16, No.1, 1997.
14. ITU-T X.435, "Message Handling System : EDI Message System," Geneva, 1991.
15. 강창구, "EDI 정보보호 서비스 분석," 제2차 안전한 EDI 관련기술 심포지움, 1996. 3.
16. 전윤호 · 이필중, "EDI 표준과 관련된 EDI 보안 서비스에 관한 고찰," 통신정보보호학회지, Vol.4, No.2, 1994. 6.
17. 이경상, "CALS 표준에 따른 EDI 보안," 정보과학회지 제13권 11호, 1995. 11.
18. 윤여웅 · 소우영 · 한근희, "안전한 CALS 구현을 위한 정보보호 기술 활용," 정보보호학술대회 발표논문집, 1997. 9.

19. 강창구 · 최용락, "개방형 분산시스템 환경의 인증 메커니즘 분석," 통신정보보호학회지, Vol.7, No.2, 1997, 6.
20. 최용락 · 강창구, "디렉토리 모델과 정보보호 서비스," 통신정보보호학회지, Vol.5, No.3, 1995. 9.
21. 정진욱, "EDI 보호(Security)," 전자공학회지, 제21권 5호, 1994. 5.
22. 김상진, "CALS/EC구축 표준모형," 한국CALS/EC 충청지부학회, 제2회 초청세미나, Oct., 1997
23. 김진웅, "전자상거래 개요 및 국내 추진현황," 한국CALS/EC 충청지부학회, 제2회 초청세미나, Oct., 1997.
24. 박성준, "전자상거래와 정보보호 기술," 한국CALS/EC 충청지부학회, 제2회 초청세미나, Oct., 1997.
25. 김춘길, "전자상거래와 한국통신의 추진전략," 충청지부학회, 제2회 초청세미나, Oct., 1997.
26. 류철철, "전자상거래를 위한 신용보증 시스템," 한국CALS/EC 충청지부학회, 제2회 초청세미나, Oct., 1997.
27. 한국통신정보보호학회 '97, "초고속 정보통신 기반 안전성 기술," 제1회 개방형보안기술과 응용 워크숍, 1997.
28 최영철 · 원동호, "An Improved Single Term Off-Line Coins," *processing of JW-ISC '97*, Oct., 1997.

Abstract

Analysis of Components Endangering Information Protection in CALS/EC

Kang suck-joo · Kim, Chang-tae

CALS(Commerce At Light Speed)/EC(Electronic Commerce) is drawing considerable interest as strategic part of efforts for computerization of the government and companies and for industry-wide innovation, using Internet and information superhighway that is widely expanding world-wide with the development of computers and information communication technology. In the current industry infrastructure, standardization is difficult but very important among the parties that want to share the added value, as external environmental components increase since the advent of computers.

However, information security technology is not permitted to be exported in light of national interest or high amount of royalty should be paid. Moreover, if we cannot fully analyze the international standard and imported technology in order to verify the safety of using them, domestic information can be exposed according to the desire of the country exporting the technology.

In particular, information security technology should be developed by ourselves, considering technology protection and export prevention policies of foreign countries. Therefore, this paper presents information security technology and standardization trends for several application fields regarding CALS/EC implementation in our and foreign countries. This paper also analyzes such trends and proposes strategic direction for standardization suited for domestic environment.