通信情報保護學會誌
第1卷, 第3號, 1991. 12

전자식 문서 교환(EDI)의 보안과 통제관리

김정희* · 김태윤*

1. 서 론

EDI(Electronic Data Interchange : 전자식 문서 교환)는 한 기업의 컴퓨터로부터 다른 기업의 컴퓨터로 표준화된 서식에 맞추어서 정보를 교환하는 과정을 말한다.

EDI를 이용함으로써 얻을 수 있는 효과는 크다. 어느 회사에서 기존에 보유하고 있던 시스템에 EDI 시스템을 연결하여 활용하게 되면 그 회사는 많은 잇점을 얻을 수 있게 된다. EDI 시스템을 도입한 회사는 거래처의 요구에 보다 신속하게 대응할 수 있고, 재고 수준이 보다 감축될 수 있으며, 다품종 소량 주문에 대처할 수 있는 능력이 향상되고, 납품업체 및 운송업체 등에 대해서도 보다 높은 반응성을 요구할 수 있게 된다. 또한 전자적으로 자금 이체가 자동으로 이루어지게 됨으로써 자금 이체 일정이 명확하게 되고, 이를 통해서 자금의 흐름 및 자금 비용의 관리가 보다 개선될 수 있다.

이러한 효과를 최대로 얻기 위해서는 부수적으로 발생되고 처리되어야 할 문제점들이 생겨난다. 이는 기업간에 거래되는 자료에 대한 신뢰성과 보안성의 문제이다. 거래 자료의 교환 처리가 보다 자동화되고 일상적인 의사결정 과정과 긴밀하게 연결되면 될수록 그것을 사용하는 회사의 컴퓨터 시스템 및 통신망 그리고 그 회사와 그 자료를 주고받거나 이를 중간에서 중계해주는 측의 신뢰성 및 보안성이 중요한 문제로 대두하게 된다.

EDI를 사용할 때 직면하게 될 위험에는 사기, 생산활동의 혼란, 회사 업무의 조작, 고객 서비스의 불균형, 의사결정의 적절성 저하, 재무 제표에 대한 신뢰성 부족, 법적인 책임, 시장 점유율 또는 경쟁력 우위의 상실 그리고 재산상의 손실 및 재난 등이 있을 수 있다.

EDI의 활용이 확산됨에 따라 기존의 업무 환경 및 응용 시스템에 대한 통제절차에 대한 재검토가 필요하게 될 수도 있다. EDI를 활용하게 됨으로써 현재의 시스템, 절차 그리고 업무수행 방법에 대해 일어나게 될 변화로 인해서 지금까지는 없었던 위험에 대해서 대비를 해 둘 필요가 있다.

따라서 본 연구에서는 EDI 시스템을 사용함으로써 나타나게 되는 보안에 대한 필요성과 문제점, 고려 사항들을 찾아서 제시한다. 그리고 전문 EDI 서비스업자의 통신망을 이용하는 경우를 살펴보면서 보안 문제의 해결에 관련된 대책들을 제시한다.

2. 보안과 통제관리 사항

EDI를 사용하게 됨으로써 해당 이용 회사 및 그 회사가 속한 업계는 많은 영향을 받게된다. EDI가 기업업무의 전략적 차원에서나 또는 일상 업무의 수행 차원에서 어떤 영향을 미칠 것인가. 그리고

* 고려대학교 전산과학과

회계 및 통제관리 측면에서 어떠한 영향을 미칠 것인가를 고려해야 한다. 따라서 통제상 다음과 같은 사항들을 고려해야 한다.

1) 업계 내의 EDI 추진 그룹에 대표자를 참여시켜 교환할 문서 및 그 양식을 결정하고 그 자료에 대한 보호 방안의 결정에 대해 의견을 반영할 수 있도록해야 한다.

2) EDI 도입에 관한 계획을 잘 세워서 기업의 사업상 목적에 부합되고 기존의 시스템과 잘 결합되어 적절한 관리적, 기술적 자원이 지원되도록 해야 한다.

3) 컴퓨터와 통신망에 대한 기존의 보안관리 대책 및 모든 개선안이 자사의 자료에 대한 부당한 액세스로부터 보호될 수 있도록 해야 한다.

4) 기존의 보안 대책이 EDI를 도입하는데 따르는 위험에 대비하기에 부적절한 경우에는 보안 대책을 적당한 수준으로 강화하여야 한다.

5) 모든 응용 시스템들이 승인받지 않은 변경이나 사고에 의한 변경으로부터 보호 받도록 해야하고 유지보수가 가능해야 한다.

6) EDI 및 EDI와 관련된 응용 시스템들이 회사의 요구 사항들에 맞게 개발되고 유지보수가 가능하도록 해야 한다.

7) EDI 시스템 및 관련 응용 시스템에 적절한 수작업 또는 컴퓨터를 이용한 통제 및 감사 기록 기능을 구비하여 문제점을 적시에 발견하고 처리할 수 있도록 한다.

8) 거래처 및 전문 EDI 서비스업계와의 사이에 법적인 책임과 의무, 절차상의 합의 사항들을 문서상으로 확인할 수 있고 적절한 법률 관련기관의 검토 대상이 될 수 있도록 해야 한다.

전략적 의미에서의 EDI 계획 수립 및 경영자층의 관심 사항을 다음과 같이 제시할 수 있다.

EDI의 도입전에 경영자층은 당면한 위험을 확인하고 적절한 통제관리 기법을 개발하기 위한 위험 분석을 실시해야 한다. EDI를 도입하게 됨으로써 영향을 받게 될 기존의 응용 시스템에 관련된 위험 수준과 새로이 발생할 제반 위험, 해당 조직내에서 계획하고 있는 EDI 활용 수준 및 유형을 살핀다. 이와 같은 위험의 결과로 인하여 조직이 받을 충격의 정도에 대한 우선 순위 결정, 대안에 대한 비용산정, 위험 대처 전략의 도출에 대한 검토 등이 이루어져야 한다.

EDI의 도입이 현재 및 미래의 기업에 미칠 영향을 고려하여 이들 부문에 EDI를 활용하기 위한 현업의 전략계획을 수립해야 하고 EDI가 기존의 관리구조 및 절차에 미치는 영향을 파악하여 기존의 시스템 업무와 통합하는 일을 검토해야 한다. 이를 위하여 EDI 전문가가 조정역으로 상담 창구 역할을 하며 기술적 조언, 안내 및 문제해결 역할을 수행해야 하고 EDI 운영에 관한 사용수준, 비용 등의 감시 관찰을 하도록 한다.

EDI 시스템의 개발 및 도입과정에서 EDI의 효과적인 관리는 필수적이며, 업계의 EDI 추진조직의 핵심 관리자가 참여하는 것이 필요하다. 새로운 시스템에 대한 도입 전후에 각각 내부 및 외부 감사인의 감사가 이루어져야 한다. EDI의 도입 초기에 거래처 및 업계추진 조직과의 접촉을 통해 기초적인 사항에 대한 사전 협의가 이루어져야 하고 계약상의 요구사항을 문서화하여야 한다. EDI 변환처리를 위해서 사용할 자료의 변환 규칙이 정해져야 하고 오류 및 장애를 파악하고 복구해야 하며 우발 사태에 대한 대비 계획이 있어야 한다. 그리고 둘 이상의 전문 EDI 중계업자를 이용하게 되는 거래자료가 있는 경우에는 EDI의 활용 촉진을 위해 표준적인 내부 인터페이스를 마련해야 한다.

그리고 적절한 백업 복구(backup recovery) 및 운영 재개 기능을 마련해서 내부 시스템이나 통신망 장애시에도 시스템 및 통신망의 계속성이 유지되도록 해야 하고 용량 계획시 EDI 처리 업무에 대한 증가에 대처할 수 있도록 계획이 수립되어야 하며, 재해복구 계획에 EDI 처리까지 포함되도록 한다. 또한 EDI에 사용되는 모든 컴퓨터 장비와 소프트웨어 및 기타 컴퓨터 시스템의 재고를 확보해 둔다.

또한 표준 계약서는 해당 국가의 EDI 지원 조직에서 제공하는 모범계약서에 근거하여 작성되어야 하며, 모든 계약 당사자가 명확하게 이해할 수 있도록 상세하게 문서화되어야 한다. 법적인 계약

서에는 EDI 통신 지침서 및 EDI 사용자 지침서를 추가하여 보충하도록 해야 하고 계약서의 효력 인정에 대한 방침 및 절차가 미리 정해져야 한다.

EDI를 도입하고 시행하기 이전에 반드시 구비되어야 할 것 중의 하나가 EDI 통신 지침서이다. 이 지침서에는 기업간의 문서 거래에 사용될 EDI 문서표준 및 통신 프로토콜이 포함된 EDI 메시지의 양식, 구조, 전송 등에 관한 방법 및 절차가 규정되어야 하며, 다음과 같은 내용에 관한 대책이 수립되어 있어야 한다.

- 송신자에 대한 정당한 인증 여부의 확인
- 메시지의 시작과 끝의 구별
- 부당한 액세스를 방지하기 위한 보안 절차
- 교환할 거래 서식 및 각 메시지에 대한 표준 구조
- 교환 주소 및 코드와 교환하는 빈도
- 특정 메시지 유형의 법적인 상태
- 최신 버젼의 문서 표준 및 통신 소프트웨어

그리고 EDI를 사용하기 전에 EDI 사용자 지침서가 작성되어 있어야 한다. EDI 사용자 지침서에는 거래처간의 EDI 자료 교환에 관한 운영 방법 및 절차 등에 관한 내용이 포함되어 있어야 하며 다음과 같은 사항 등이 규정되어 있어야 한다.

- 처리의 중단 및 지연시에 대비한 합의된 절차
- 암호화 키 및 알고리즘 등을 포함한 거래처간에 적용할 보안 절차
- 변환 소프트웨어의 버전 갱신 절차
- 거래 자료 수신 확인 방법
- 어떤 자료를 얼마동안 보관하는가에 대한 문제
- 종이 문서 전달의 정지 등에 관한 사항들
- 응용 시스템의 인터페이스

3. 시스템 통제관리와 체크리스트

시스템의 통제관리 방법을 평가할 때에는 EDI를 도입하게 됨으로써 발생하게 될 통제관리 처리가 무엇인가를 파악해야 하며, EDI를 도입함으로써 영향을 받게 되는 기존의 시스템에 대한 통제관리 방법에 대한 적절성도 검토되어야 한다. 그리고 거래 자료가 수신자료인가 송신 자료인가에 따라 적용되는 통제관리 방식이 달라져야 한다.

EDI를 사용하게 되는 상황에서는 거래 자료가 현업에 미치는 영향이 매우 커진다. 따라서 거래 문서에 대한 보다 빠른 반응을 요구하게 되므로 EDI의 처리 싸이클상 초기에 발생되는 문제들, 특히 기업 내부로 들어오는 거래 자료에 대하여 발생할 수 있는 문제를 조기에 파악하여 효율적으로 대처하는 것이 요구된다. 문제가 발생한 후에 이 문제점을 해결하기 위한 통제관리를 하는 경우에는 결과에 대처하기에 시간상으로 너무 늦을 뿐만 아니라 이미 발생되어 버린 상황에 대한 책임을 질 수 없게 된다. 따라서 사전 관리의 필요성이 더욱 커지게 된다. 다시 말하면 인간이 처리과정에 개입하는 일이 줄어드는 대신에 자동화된 통제관리 기능이 그만큼 더 지능적인 것이 되어야 할 것이다.

우선 각각의 거래 자료에 따라 발생될 수 있는 위험 요소들을 수신 거래 자료와 송신 거래 자료로 구분하여 분석한다.

수신 거래 자료의 경우에 있어서 거래처로부터 유입되는 거래 자료의 유실 또는 중복이 있을 수 있고, 이에 따라 잘못된 수신자료를 근거로 한 대응이 적절하지 못한 경우가 발생된다. 거래 자료가 회계기록에 정확하게 기재되지 않을 위험성이 있으며, 거래처의 요구에 적절하지 못한 행동을 하거나 전혀 반응을 하지 못할 위험성도 존재한다. 그리고 부당하거나 부정확한 혹은 송신측으로부터 승인받지 않은 수신자료를 바탕으로 불필요하거나 해서는 안될 일을 처리하게 될 수도 있다. 반면에 송신 거래 자료의 경우에 거래처에 대한 요구에 대하여 거래 상대편에서 적시에 적절한 조치를 취하지 않거나 전혀 반응이 없을 수 있으며, 이에 따라 거래처에 대한 중복적인 요구가 발생한다. 그리고 부당하거나 부정확한 혹은 승인받지 않은 자료를 송신함으로써 상대방이 이를 근거로 한 불필요한 작업을 처리하게 될 수도 있다.

이러한 위험 요소들을 예방하기 위한 통제관리와 이에 관련된 고려 사항들을 다음과 같이 제시할 수 있다. 수신 거래 자료인 경우에는 거래 자료에 대한 중복이 없는가 확인하고 변경 또는 수정없이 수신되었는지 확인한다. 그리고 정당하게 승인된 자료인가를 확인하고 비정상 거래 자료일 경우에는 별도로 관리해야 할 필요가 있다. 거래 상대방 시스템으로의 자료 전달시 중복 전달이 없이 올바로 전달되도록 하고 각각의 거래 자료가 응용프로그램으로 전달되기 전에 부정확하거나 잘못된 변경이 가해지지 않도록 한다. 내부 처리가 이루어지기 전에 부당하거나 비정상적인 거래 자료를 발견 및 조사할 수 있어야 한다. 한번 수신한 거래 자료는 임시 화일이나 PC에 보관할 때 주의해야 한다.

또한 송신 거래 자료의 경우에는 송신할 모든 거래 자료가 EDI 서식으로 단 한번 작성되었는지 확인하고 정당하게 승인받은 거래 서식만이 EDI 서식으로 작성되도록 한다. 이를 위해서 거래에 필요한 서식은 정확하게 그리고 필요한 시점에 작성되도록 한다. 작성된 거래 서식은 중복없이 전송되도록 하고 목적한 거래처에 적절한 시간에 전송되도록 한다. 또한 EDI 거래 서식 화일을 충분한 기간동안 적절한 양식으로 보관함으로써 과세 및 법률적인 문제와 EDI 거래 서식과 관련된 의문 및 분쟁의 해결에 대비할 수 있도록 하여야 한다. 문서 표준은 EDI를 이용해서 전송하려고 하는 모든 거래서식에 대해 해당업계에서 인정한 것을 사용한다. 필요한 경우 메시지의 완전성 및 정확성을 보장하기 위한 통제관리상의 요구사항에 부합되는지에 대하여 EDI 시스템 및 EDI에 관련된 모든 응용시스템을 경영자층이 승인한 계획 및 절차와 방법론에 따라 개발 또는 수정하도록 한다. 프로그램의 변경에 대한 통제관리 절차를 적용함으로써 최종적으로 승인된 소프트웨어만을 실무에 적용시키도록 해야 한다.

따라서 EDI 시스템의 통제관리를 위하여 필요한 체크리스트를 다음과 같이 수신 거래 서식과 송신 거래 서식으로 구분하여 제시할 수 있다.

수신 거래 서식의 경우에는 완전성과 정확성을 기하기 위하여 처리전에 오류가 있으나 부당한 거래 서식을 찾기 위한 편집확인을 한다. 거래서식의 적절성, 정당성 및 기타 사항의 확인을 위한 추가적인 자동 확인 기능에 대해 검토하고 보다 복잡한 문제에 대해서는 전문가 시스템 등의 활용도 고려한다. 거래처에 대한 상세한 자료를 근거로 송신자의 정당성을 확인하고 임시 화일이나 전송 중인 자료에 대한 보안 조치를 함으로써 변조되는 일이 없도록 하며 메시지 표준 양식으로부터 자료가 완전하고 정확하게 내부 시스템에서 사용할 수 있는 자료양식으로 변환되는가를 확인한다. 송신 거래 서식의 경우에는 모든 거래 서식들이 적시에 작성될 수 있도록 효과적인 통제관리 기능을 마련하여야 한다. 그리고 모든 송신 거래 서식이 작성된 시점과 전송시점 사이에서 변경되는 일이 없도록 한다. 또한 송신 거래 자료에 대한 적절한 승인 절차를 수행한다.

모든 사용 기록 및 보고사항 등 중요한 문제를 일으킬 수 있는 것으로 판단되는 거래 자료를 신속하게 찾아내어 그에 따른 행동이 일어나기 전에 조치를 취할 수 있도록 찾기 쉬운 양식 및 매체에 보관하고 정기적으로 예의 상황보고 내용을 검토하며, 거래처의 수신확인 및 전문 EDI 서비스제공업자의 보고서와 대조 확인을 위한 감사 및 관리용 기록을 마련한다.

4. EDI 사용자 인증

EDI 메시지에 대한 사용자 인증이라는 것은 자료를 교환하고 있는 거래 상대방이 올바르게 승인된 거래처이며, 교환하는 자료도 정당한 자료라는 것을 보증하는 작업이다. 일단 EDI를 전업무에 걸쳐 활용하는 상황에 이르게 되면 더이상 서명이 된 종이 문서는 사용할 수 없게 되기 때문에 사용자에 대한 인증이라는 것은 EDI 시스템의 사용에 있어서 반드시 필요로 되는 매우 중요한 일이 된다.

사용자의 인증에 대한 통제는 송수신 거래 자료 모두에 대해서 이루어져야 하며, 특히 송신 거래 자료에 대해서는 사내의 응용 시스템에 대한 전반

적인 보안 및 특정 부문에 대한 보안 조처까지 고려해야 한다.

사용자에 대한 인증이 잘못되면 오류에 대한 법적인 책임을 입증할 수 없게 되고, 불완전한 자료의 송수신을 초래하며, 인증되지 않은 거래 자료가 유입될 수 있게 된다. 자료는 반드시 받도록 되어 있는 사람에게만 공개되도록 하고 부당한 메시지는 그것에 따른 행동이 개시되기 이전에 발견하여 삭제하도록 하여야 한다. 메시지가 최종 목적지에까지 손상이나 변경없이 도달되도록 하고 승인된 사용자만이 거래 자료를 작성하도록 하며 암호화 키는 안전하도록 비밀이 보장될 필요가 있다. 또한 EDI 시스템을 사용할 수 없는 경우에도 메시지에 대한 적절한 사용자 인증 방법에 따른 처리가 이루어지도록 하여야 한다.

EDI를 이용하여 거래 자료를 전송할 때에 받는 사람은 그 자료가 정당하고 승인 받은 거래처로부터 오는지 확인하는 일이 중요하므로 위험성이 높은 거래 자료에 대해서, 수신자는 즉시 그 자료가 유효한 것인지 또는 전송시점과 수신 시점 사이에서 자료의 변경이 없었는지를 확인해야 한다. 이를 위해서 다음과 같은 사항들이 검토되어야 한다.

- 메시지에 대해서 디지탈 서명 또는 이와 유사한 방법을 적용한다.
- 표준 문서 헤더를 이용하는 문서에 인증 부분을 추가한다.
- 운영되는 유효 거래처 정보(계정 번호, 여신한도, 핵심 정도 등)표를 통제관리하에 작성하고 운영할 수 있도록 한다.
- 전문 EDI 서비스업자를 이용하여 효과적으로 거래처를 선별한다.

또한 승인된 사용자만이 거래 자료를 초기에 작성할 수 있도록 하기 위하여 다음과 같은 통제관리 절차의 수행이 필요하다.

- 회사 내에서 특정 EDI 거래 자료를 작성할 수 있는 사용자의 권한을 제한한다.
- 위험도와 보안의 필요성이 높은 거래 자료에 대해서는 작성 책임자와 전송 책임자를 따로 둔다.
- 책임 소재 파악 및 감사 기록이 가능하도록 한다.
- 디지탈 서명, 중복 승인, 스마트 카드 등의 사용 방법을 고려한다.
- 자동적으로 거래 자료가 작성되는 경우에는 사고의 발생시에 취할 수 있는 적절한 승인 과정을 마련하여 둔다. 그리고 모든 지급 거래 문서는 별도의 화일에 기록해 두었다가 전송전에 확인하여 승인을 하도록 한다. 특히 경영자층은 거래 은행과 지급 거래 문서의 자동 작성방법에 대해서 검토하여야 한다.
- 기업간의 문서 거래 주기 내에서 주문 입력 및 승인, 물품 입고 확인, 지급 승인 등의 업무 책임을 서로 다른 사람에게 맡기도록 한다.

위험성이 높은 거래 자료를 변경 또는 변조로부터 보호하기 위해서는 메시지 인증 코드를 이용해서 거래 자료의 제반 키 및 자료 항목을 검증하여야 하며, 인증이 되지 못한 거래 자료는 기록을 남겨 두고 즉시 확인하여 적절한 조치를 취해야 한다.

EDI 시스템을 사용할 수 없게 될 때에는 전화나 팩시밀리 전송 등과 같은 다른 인증 방법을 마련해 두어야 한다. 그러나 이런 장비들은 안전성을 충분하게 보장할 수 없기 때문에 비밀 자료나 중요 자료가 아닌 경우에만 사용하도록 하고 그외에는 사용을 억제하도록 한다.

시스템 내에 타당성 검증 및 대조 확인 기능을 갖추어 두어야 하며, 암호화 기법을 사용하는 경우에는 효과적인 키 관리 기법도 마련하여야 한다.

5. 컴퓨터 내부에서의 통신상에서의 보안 관리

5. 1 컴퓨터 내부에서와 보안 관리

오늘날에 있어서 보안 문제는 중요한 문제로 부각되고 있다. 화이트 컬러범죄, 산업 스파이 행위, 컴퓨터 바이러스 그리고 인간의 단순한 실수만으로도 컴퓨터 시스템이 커다란 위험에 처할 수 있게 된다. 그러므로 컴퓨터에 대한 의존도가 높아질수록 보안의 필요성은 더욱 커지게 된다. 특히 EDI를

도입하게 되면 보안의 중요성은 한층 더 중요하게 된다. 그러므로 다음과 같은 통제 관리 사항을 고려해야 한다.

각각의 EDI 거래 자료 유형에 따라 필요하고 적절한 보안 관리 대책 수준을 결정하여 일관성 있게 적용하고 EDI 및 EDI와 관련된 모든 소프트웨어에 대한 논리적 액세스를 제한한다. 또한 EDI 및 EDI 관련 거래 자료를 사기나 오류로부터 보호할 수 있도록 이에 관련된 주요 기능을 두사람 이상에게 분담시키고 모든 송신, 처리, 수신 거래 자료에 대한 액세스 내용을 감사용 기록으로 남겨둔다.

논리적 보안 관리를 위하여 각각의 거래 자료에 관련된 위험의 정도를 파악하고 핵심 부분에 대하여 우선적으로 조치를 취하며 EDI와 관련하여 추가적으로 필요한 통제관리 사항을 문서화하고 준수하도록 한다. 수신 거래 자료인 경우에는 수신 시점부터 시스템 갱신시까지, 또 송신 거래 자료인 경우에는 문서 작성에서부터 송신 시점까지 자료가 보호될 수 있도록 한다. 운영 체제가 적정 수준의 보안 기능을 제공하는지, 또 운영 체제가 제공하는 핵심 보안 기능이 일관성 있게 적용되고 있는가를 확인해야 한다. 자료 및 거래 자료에 대한 액세스를 제한하기 위해서는 정기적인 패스워드의 변경, 마스터 화일 레코드, 로그온 시도 횟수의 최소한도 제한, 자동 로그아웃 처리 등도 고려해야 한다. 이러한 전체적인 보안 환경이 여러가지 EDI 처리 대상 거래 자료 유형에 관련된 위험에 대해 효과적으로 대처할 수 있는지도 확인해야 한다. 그리고 물리적인 보안 조치가 양호한가를 확인하여야 하며, 이는 특히 PC 자체를 통신 노드로 사용하는 경우에는 반드시 필요하게 된다. 하드웨어 또는 장비의 중복성, 물리적 위치 및 접근가능, 정전 방지, 자료 보관 및 외부 백업, 보험 등에 유의한다.

EDI 및 EDI 관련 시스템과 컴퓨터 시스템에 관련된 모든 액세스에 대한 기록의 감사 및 관리를 수행한다. 보안 위반이 예상되는 문제를 조속히 찾아내고 즉시 조치할 수 있도록 한다.

5. 2 통신상에서의 보안 관리

업무상의 필요 때문에 근거리 통신망(LAN) 및 광역 통신망(WAN)에 자사의 컴퓨터 시스템을 접속하는 기업의 수가 늘어나면서 통신 회선 상에서의 보안관리는 매우 높은 관심을 불러 일으켜 왔다. 특히 EDI는 통신망의 보안을 요구하는 또하나의 요인이 되고 있다. 따라서 어떤 통신 프로토콜 표준(X. 25, X. 400)을 사용할 것인지, 어떻게 도입할 것인지, 선정한 표준 중 어떠한 기능을 도입할 것인지, 어떤 매체와 장비를 도입할 것이지, 또한 필요로 하는 보안 관리 장비 및 소프트웨어는 어떤 것이 있는가 등을 고려하여야 한다.

통신상의 보안 관리가 이루어지지 않았을 때 나타날 위험 요소로는 승인 받지 않은 메시지가 송신 또는 수신될 위험성, 메시지가 잘못 전송될 위험성, 전송 과정에서 메시지가 유실, 변경 또는 중복될 위험성, 바이러스가 컴퓨터 시스템에 침입할 위험성, 통신망의 장애성, 통신망 상의 지연 또는 오류성, 중요 메시지의 전달 지연성 등이 있을 수 있다.

이러한 내용의 통제를 위하여 고려하여야 할 사항들을 다음과 같이 제시할 수 있다. 대외적으로 중요하거나 비밀 자료로 분류된 자료에 대해서는 통신망 상에서 승인없이 공개되지 않도록 보호 조치하고 교환되는 모든 메시지에 대하여 지나친 지연이나 유실, 또는 중복이 없도록 한다. 바이러스가 컴퓨터 시스템에 전송되어 들어오지 않도록 조치하고 통신 매체 및 장비를 승인받지 않은 액세스로부터 안전하게 보호하고 EDI 통신의 두절시에도 거래를 계속할 수 있도록 조치한다.

EDI 통신 보안 관리를 위하여 고려할 각각의 세부사항들에 대한 보다 상세한 내용을 제시하면 다음과 같다.

1) 보 안

터미널과 컴퓨터간 그리고 컴퓨터와 외부 통신망 사이에 안전한 물리적 선로를 연결하여 부당한 도

청을 막고 통신 제어 장치 및 다중화 장비에 부당하게 액세스하는 일을 막는다. 패킷 통신망을 이용하는 경우에는 EDI 전송을 이용하는 사용자들로 만들어지는 폐쇄 이용자 집단의 구성을 고려하고 ISO와 같은 기구에서 제안한 보안 표준이 있는 메시지 처리 시스템 등을 활용한다. EDI 전용 통신 프로토콜인 X. 435에서 정의하고 있는 보안 서비스는 다음 표 1과 같다.

MHS(Message Handling System)는 공용키 암호화(Public Key Cryptography) 방법과 해쉬 함수(Hash Function)를 메시지 내용에 적용함으로써 authentication, integrity, confidentiality 등의 보안 기능을 제공한다.

표 1. X.435 서비스 내용과 권고

origin authentication	: X.402
EDIM responsibility authentication	: X.435
proof of EDI notification	: X.435
proof of retrieval	: X.435
proof of transfer	: X.435
secure access management	: X.402
data confidentiality	: X.402
data integrity	: X.402
non-repudiation	: X.402
non-repudiation of EDIM responsibility	: X.435
non-repudiation of EDI notification	: X.435
non-repudiation of retrieval	: X.435
non-repudiation of transfer	: X.435
non-repudiation of content	: X.435
message security labelling	: X.402
security management services	: X.402

2) 암호화

위험성이 특히 높은 거래 자료에 대해서는 암호화의 필요성이 더욱 크게 대두된다. 그러므로 암호화 대상이 되는 메시지, 메시지 내용 중 암호화가 필요한 세그먼트 그리고 자료의 암호화에 사용할 알고리즘 등에 유의하여 DES나 RSA 같은 일반적인 암호화 기법들의 사용을 고려한다.

3) 검 증

적절한 기법을 활용하여 수신 거래 자료가 부당한 것으로 취급받지 않도록 한다. 이를 위하여 거래 서식 유형 혹은 거래처별로 고유의 일련 번호를 부여하여 확인할 수도 있다. 거래처로부터 받은 거래 자료에 대해 자동적으로 수신 확인을 작성하도록 Hash Total, Control Total, Full Content Acknowledgement 등의 기법을 사용한다.

4) 감사 기록

분쟁의 경우에 대비하여 송수신 메시지를 교환 자료 형태 그대로 작성하여 보관하고 감사 기록 자료에는 레코드마다 인증 코드를 적용하여 부당한 조작이 불가능하게 한다. 주요 자료를 독립적인 외부의 전문 EDI 서비스 제공업자에게 전송하여 그곳에 보관하도록 하고 통신 과정상의 전송 오류가 있을 때에도 적절한 복구가 가능하도록 필요한 절차를 마련한다.

5) 운영상의 통제관리

거래 서식의 전송에서 발생될 수 있는 시간상의 지연을 방지하기 위해 이에 필요한 적절한 통신망 용량을 확보하고 전송시 발생되는 오류를 줄이기 위해 전송 오류시 전송 재개 및 복구 기능 측면을 고려한 통신 프로토콜을 사용한다. 또한 선정한 통신망 및 프로토콜의 신뢰성을 검토하고 장애시기에 대비하기 위하여 장비 및 전송 매체를 중복 구성한다. 모뎀 및 기타 통신 장비에 대한 다이얼 보호 장치를 하고 다른 장소로 재전송할 수 있는 기능을 확보한다. 통신 전문가를 지정 또는 활용하고, 관련 운영 요원들에 대해서 적절한 교육과 훈련을 실시한다.

이상과 같은 보안 대책 및 관리하에서 EDI 시

스템을 활용하는 사용자는 적시에 메시지 저장소에 저장된 메시지를 인출하거나 임의의 시간에 메시지 저장소로 메시지를 전달하도록 한다. 이런 메시지 인출 및 전달에 있어서의 최대 허용 지연 시간은 계약서 상에 명시되어 있어야 한다. 또 사용자는 정기적으로 상대방 거래처가 메시지 저장소에서 메시지를 인출하여 갔는가를 확인하고, 수신 메시지에 대해서는 수신 확인을 하는 것이 바람직하다. 사용자는 관리 기능에 대한 임무를 자신이 스스로 수행하도록 하고 중계자가 자신의 패스워드, 거래처 관련사항의 설정 및 유지 관리 등의 업무를 하지 못하도록 한다. 사용자는 전문 중계 서비스업자와의 계약 체결 이전에 해당 서비스업자와의 보안 기능에 대한 외부 감사인의 감사 보고서를 검토하도록 한다.

6. 전문 EDI 서비스업자 통신망 및 우편함 보관상의 보안 관리

EDI를 도입할 때 유효하며 완전하고 승인된 거래 자료들을 교환하기 위해서는 적어도 한군데 정도의 전문 EDI 서비스업자를 이용하는 것이 좋다. 이 경우에는 거래 자료를 외부로부터 보호하기 위해서 이들 전문 서비스업자의 자체 보안 관리 능력에 의존할 것이다. 이런 경우에 보안상의 안전을 확보하기 위한 가장 좋은 방안은 이들 전문업체와의 사이에 계약을 맺어두는 일과 전문업체들이 정기적으로 외부 감사인에 의해 감사를 받도록 하는 것이다.

이러한 EDI 보안 및 통제관리를 잘못했을 때 발생될 수 있는 위험 요소들을 보면 다음과 같다.

- 거래처 사이 또는 전문 사업자의 통신망 사이에서의 거래 자료 유실
- 전문 사업자의 통신망 또는 우편함 상에 보관되어 있는 경쟁상 중요 자료 또는 비밀 자료의 공개
- 전문 EDI 서비스업자의 통신망 상에서 고의로 인한 문서의 변경 및 변조
- 잘못되거나 승인을 받지 않은 거래 자료의 우편함 내로의 유입
- 운영상의 실수 및 장비의 장애 등으로 인한 거래 자료의 전송 지연
- 우편함에서의 메시지 인출 지연
- EDI 서비스에 대한 잘못된 비용 부과

전문 EDI 서비스업체는 물리적, 논리적으로 우편함 서비스의 보안성을 확인하고 부당한 전송 자료에 대한 신속한 조치를 취한다. 통신망 및 우편함에 대한 접근이 통제되고 있는가를 확인하고 교환되는 거래 자료에 관하여 적절한 기록을 일정 기간 보관하고 있는지를 확인할 필요가 있다.

전문 EDI 서비스용 통신망에서는 적절한 수준의 보안 관리 기능이 갖추어져야 하며 이러한 사항에 대해서는 사용자들 스스로도 보호를 위하여 보안 관리 기능을 갖추어야 한다. 전문 서비스업자의 보안 및 운영에 있어서 미비한 부분이 있을 경우에는 사용자 측에서 추가적인 통제관리 절차를 보완하여야 한다.

전문 EDI 서비스업자는 다음과 같은 사항을 지원해야 한다.

- 통신망에의 접속을 요구하는 모든 사용자에 대해 그 정당성을 확인한 후에 접속을 허용해야 한다.
- 인증 절차를 통과하지 못한 사용자가 있을 경우에는 즉시 이에 대한 확인 및 조치를 취한다.
- 모든 다이얼의 접근에 대한 기록을 일정 기간 남겨야 하고 통신망에 관련된 모든 패스워드를 주기적으로 갱신한다.
- 승인된 사용자만이 접근할 수 있도록 하드웨어 및 소프트웨어적인 장치를 이용한다.
- 메시지가 올바른 순서로 수신 목적지에 도달할 수 있도록 하기 위해 자동데이타 패킷 순서 확인 기능이 가능하도록 한다.
- 요구에 따라 메시지를 다른 장소로 재전송할 수 있는 기능을 확보해야 한다.
- 장애시에 대비한 통신망 및 컴퓨터 장비에

대한 복구 절차 및 장애 방지조치를 한다.

• 패스워드 변경의 승인, 서비스업체 직원의 우편함에 대한 접근 통제, 우편함에 대한 접근 수준 및 방법의 규정 등에 관한 공식적 절차를 마련한다.

전송 자료가 2개 이상의 전문 중계업자의 통신망을 거쳐야 되는 경우에 사용자는 이 두 중계업자 사이의 통신망 연결 부분에서 자료의 유실 여부를 확인할 수 있는 수신 확인 서비스의 이용을 충분히 고려해야 한다.

또한 감사 기록에 관하여 특별히 중요한 내용인 경우에는 다음과 같은 사항도 고려해야 한다.

• 메시지 내용을 종이에 인쇄하여 보관하는 방안

• 이런 거래 자료를 파악 검토할 수 있는 추가적인 통제관리 방안 마련

• 부당한 메시지로 인한 이익의 감소 및 예상되는 법률상의 책임에 대한 보험 처리

• 중요하거나 고가의 거래 내용을 담고 있는 메시지에 대해서는 별도의 등기를 함으로써 공증 감사 기록을 남길 수 있도록 한다.

그리고 전문 EDI 중계 서비스업자는 크게 다음과 같은 네가지의 보고서를 제공하여야 한다. 전송이 이루어졌으나 수신 거래처에서 수신하지 않은 문서에 관한 미수신 메시지 보고서, 일정 기간동안 특정 거래처로 발송한 문서에 대한 송신자 상태 보고서, 모든 수신 문서에 관한 수신자 상태 보고서 그리고 요금 내역서 등이다.

전문 EDI 중계 서비스업자는 사용하는 소프트웨어의 완전성을 승인 받아야 하며 자사의 서비스를 받는 모든 업계에 대한 최신 표준을 지원해야 한다. 또한 모든 소프트웨어 개발에 있어서 적절하고 합리적인 개발 표준을 따라야 하고 소프트웨어의 새로운 버젼을 내놓을 경우에는 적절한 통제절차를 밟도록 한다.

전문 EDI 중계 서비스업자는 독립된 감사인으로부터 주기적으로 보완 관리 감사를 받아서 그 결과를 사용자에게 보고하여야 한다. 이 보고에는 논리적, 물리적 그리고 통신망의 보안 관리 및 통제에 관한 사항은 물론 소프트웨어의 개발 및 메시지 표준의 변경, 우발 사태에 대한 절차 등도 포함되어야 한다.

7. 결 론

컴퓨터 통신망을 이용한 EDI 시스템을 활용함으로써 얻을 수 있는 잇점이 많이 있다. 그러나 이러한 잇점을 얻기 위해서는 부수적으로 여러가지의 문제들이 발생된다. 이러한 문제점들로는 기존 시스템과의 유기적인 결합여부, 기업의 업무처리과정의 변화, 업무 수행 방법의 변화 그리고 새로운 형태의 보안 대책의 필요성 등이다.

EDI 시스템을 사용함으로써 기업 업무에 있어서 인간이 관여할 부분이 적어지는 만큼 그에 상응하는 만큼의 자동화된 통제관리 기능이 그만큼 더 지능적인 것이 되어야 할 것이다.

기존의 업무 처리에 많은 변화를 가져오게 되는 EDI 시스템의 사용은 통신회선 상의 보안 문제 뿐만 아니라 시스템 자체의 사용에 대한 보안과 메시지에 대한 보안 그리고 시스템의 사용자에 대한 인증 문제 등이 따르게 된다.

본 연구에서는 이처럼 EDI를 활용함으로써 발생되는 문제점 중에서 특히 보안에 관한 문제를 해결하기 위하여 필요한 고려사항을 제시하였다. 컴퓨터 내부에서의 논리적, 물리적 보안관리, EDI 시스템 사용자에 대한 인증 대책을 제시하고, X.435와 MHS가 제공하는 보안 기능, 전문 EDI 서비스업자가 제공하는 보안 기능 등 통제관리의 방안들을 강구하여 제시하였다.

그러나 이 연구에서 제시된 방안들을 실제적으로 구현하는데는 많은 기술적인 어려움이 따르게 될 것이다. 그리고 EDI 사용자 인증의 문제 또는 거래 서식에 대한 논쟁이 발생하였을 때에 법적인 처리 문제 등에 관해서는 각 기업간의 합의는 물론 정부 차원에서의 법률적인 조치가 필요하게 된다. 앞으로의 연구 과제로는 보안 문제의 해결로 인하여 EDI 시스템의 사용에 불편함을 느낄 수 없도록 여기에서

제시된 여러가지 방안들을 실제적으로 구현하는 것이다.

참고문헌

1. 김태윤, 전자거래정보교환-EDI. 집문당. 1991.

2. 김태윤, "EDI 도입의 필요성," 한국경영과학회, 1990. 11.

3. 김태윤, "EDI 표준화 및 소프트웨어 개발," 한국정보과학회, 1991. 1.

4. 김태윤, "EDI 소프트웨어 설계 및 개발," 한국경영과학회, 1991. 4.

5. 김태윤, "Stand-Alone PC 환경하에서의 EDI 변환처리 시스템의 설계 및 구현," 한국정보과학회, 1991. 4.

6. 김태윤, 데이타통신과 컴퓨터통신-LAN, VAN, ISDN, 집문당, 1990.

7. Horton Sorkin, "An Introduction to EDI Security Standards," EDI FORUM, 1990.

□ 著者紹介

金 泰 潤(正會員)

고려大學校 산업공학과 졸업
미국 Wayne State University 석사
미국 Auburn University 박사
현재 고려大學校 전산과학과 교수

金 貞 姬

고려大學校 졸업
현재 고려大學校 교육대학원 재학중
연구 분야 : EDI, 컴퓨터 네트워크