EDI 보안 관리 기능 영역

o
박태규*, 강창구**, 김대호**

*한서대학교 전산정보학과, **한국전자통신연구소

Security Management Functional Areas for EDI

Tae-Kyou Park*, Chang-Goo**, Kang, Dae-Ho Kim**

*Hanseo University, **ETRI

요 약

보안 관리(Security Management)는 매우 광범위한 주제이다. EDI 망에서의 보안 관리는 목적하는 보안 정책 즉, 원하는 보안 서비스, 적용할 보안 메카니즘, 보안 수행 절차, 기반을 이루는 보안 구조, 사용 오류, 침입 시도 등의 보안에 관한 모든 사항을 관리하는 것으로 정의할 수 있다. 보안 관리의 범위는 EDI 망에서의 보안 구역(Security Domain) 단위로 구분되며, 이 보안 영역은 원하는 보안 정책을 적용하는 대상 구역이 된다. 본 논문에서는 ITU-T X.800(또는 ISO/IEC 7498-2)의 표준화에 기반을 둔 보안 영역 내에서 개발되고 있는 안전한 EDI 망에서의 보안 관리 기능 영역을 위한 정의, 범위, 요구 사항을 시스템 보안 관리, 보안 서비스 관리, 보안 메카니즘 관리, 관리 자체의 보안, 일반적 보안 관리 사항 등 5가지 범주로 나누어 다루며, 표준화 내용, 관리 도구 등을 다룬다.

1. 서론

컴퓨터를 이용한 기업, 국가 기관, 단체 등의 전자 문서 교환에 있어 중요한 정보의 저장, 처리, 전송 등이 필요함에 따라 EDI 망을 구성하여, 그 망에서의 중요한 정보를 안전하게 보호하기 위한 많은 방법들이 연구되고 있다. EDI 망의 보안 관리 기능은 OSI에서 정의한 다음의 5가지 관리적 영역 중 보안 관리 영역에 해당된다[20]. OSI에서 정의하는 5가지 관리적 영역은 첫째, 결함 관리(Fault Management)로, 망의 문제 또는 결함을 찾아내고 격리시키며, 해결하는 절차를 의미한다. 둘째, 계정 관리(Account Management)로, 망 자원에 대한 개인 사용자와 그룹 사용자의 이용도를 추적하여 사용 요금을 산정하는 행위를 의미한다. 셋째, 구성 관리(Configuration Management)로, 망을 구성하는 중요 장비를 확인하고 설치하는 절차를 말한다. 넷째, 성능 관리(Performance Management)로 망의 하드웨어, 소프트웨어 및 미디어의 성능을 측정하는 행위를 말한다. 마지막으로 보안 관리(Security Management)는, 망의 정보에 대한 통제를 통하여 중요 정보를 보호함을 의미한다. EDI 망에서의 보안 관리란 EDI 망에 연결된 장치 내에서 전송, 저장되는 중요한 정보에 대하여 통제를 가함으로써 그 정보를 안전하게 보호함을 의미한다. 중요한 정보라 함은 어떤 조직에서 안전하기를 원하는 데이터로서 이를테면 주문서,

계약서, 협정서, EDI 관리 정보 등에 관련된 것일 수 있다. 일반적으로 네트워크 보안 관리는 네트워크 관리자로 하여금 여러 가지 방법에 의해서 중요한 정보를 보호하도록 할 수 있다[1]. 이를테면, 조직의 내부 및 외부 사용자에 의한 호스트와 네트워크 장치에의 접근 통제, 자료의 비밀성 및 무결성 유지, 보안 위반 시도나 실행에 대하여 관리자에의 통보 등이다. 보안 관리의 목적은 첫째, 망에서 목표로 하는 보안 정책 지원을 위한 보안 서비스 생성, 삭제 및 제어, 둘째, 보안 메카니즘 생성, 삭제 및 제어, 셋째, 보안 관련 정보 분배, 넷째, 보안 관련 사건보고 등으로 정의할 수 있다. 한편 EDI 망의 보안 관리 기능은 EDI 자체가 국제적으로 표준화된 문서 교환망임을 고려할 때 네트워크 보안 표준인 ISO/IEC 7498-2(Security Architecture)[4], ITU-T X.800(Security Architecture)[20], ISO/IEC 7498-4(Management Framework)[5] 등의 표준을 따라야 한다.

2. EDI 보안 관리 활동의 범주(categories)

EDI 보안 관리 활동은 다음의 4가지 범주로 크게 나눌 수 있다[3]. 첫째, 시스템 보안 관리(System Security Management), 둘째, 보안 서비스 관리(Security Service Management), 셋째, 보안 메카니즘 관리(Security Mechanism Management), 넷째, 관리 보안(Security of Management) 등이다.

2.1 시스템 보안 관리(System Security Management)

EDI 망의 전반적 보안 정책을 관리하기 위해서는 하드웨어, 소프트웨어의 변화에 따라서 목적하는 보안 정책을 유지함과 아울러, 적용할 보안 기능의 설치, 유지, 운영, 그리고, 이의 수정 및 유지 시 일관성 있는 관리, 타 EDI 관리 기능과의 상호작용(Interaction), 보안 서비스, 메카니즘 관리와의 상호작용, 사건 처리 관리(Event Handling Management), 보안 감사 관리(Security Audit Management), 보안 회복 관리(Security Recovery Management) 등이 필요하며, 보안 감사 관리시 많은 자료의 양에 따른 성능 및 용량도 반드시 고려[14]해야 한다. 이러한 시스템 보안 관리의 표준화는 보안 경고보고 기능 표준(Security Alarm Reporting Function Std : ISO/IEC 10164-7[16](또는 ITU-T X.736)), 보안 감사 추적 기능(Security Audit Trail Function : ISO/IEC 10164-8[17](또는 ITU-T X.740))을 따라야 한다.

2.2 보안 서비스 관리(Security Service Management)

개발되고 있는 안전한 EDI 망에서 목표로 하는 보안 서비스는 총 27개 서비스[15]로, 다음은 이를 관리함에 있어 수행되어야 할 전형적인 활동들을 나타낸다.

① 서비스의 목표 보안의 결정, 할당 ② 보안 메카니즘의 선택, 규칙 할당, 유지 관리
③ 사용 가능 보안 메카니즘의 협상 ④ 보안 관리 기능을 통한 특정 메카니즘 호출
⑤ 타 보안 서비스 관리 기능과 보안 메카니즘과의 상호작용

이를테면 거래 자료의 비밀 등급의 구분(Multilevel Security Label)의 여부에 따른 해당 접근 제어 모델 및 메카니즘 선택, 사용자에 따른 메카니즘 사용 가능 여부, 이의 보안 관리를 위한 특정 메카니즘의 호출 가능 여부 등을 결정 및 할당 관리가 수반되어야 한다. 보안 서비스의 관리는 크게 두 가지 방법으로 나누어 구현될 수 있는데, 하나는 프로파일(Profile)을 이용 방법으로 이는 관리자, 관리 기능에 필요한 지역(Local) 및 원격(Remote)의 정보를 입력하여 파일 또는 데이터 베이스로 특정 개체(Entity)에 대한 보안 특성 등을 나타내어 여러 상황에 따른 운영 절차

를 규정하는 방법이다. 또 다른 하나는 파라메터(Parameter)를 이용하는 방법으로 프로그램 상에 사용자 ID 등의 식별 정보, 인증 정보, 상태 정보, 접근 제어 정보와 여러 경우의 문턱 값, 암호화 키 관리 정보, 기본값 및 사건 로깅 정보 등을 설정하는 방법이다.

2.3 보안 메카니즘 관리(Security Mechanism Management)

보안 메카니즘은 EDI 망에 적용할 수 있는 구현 방법으로서, 크게 암호화 관리(Encryption Management), 디지탈 서명 관리(Digital Signature Management), 접근 제어 관리(Access Control Management), 키 관리(Key Management), 데이타 무결성 관리(Data Integrity Management), 실체 인증 관리(Entity Authentication Management) 등 6가지로 대별할 수 있다[15]. 암호화 관리는 키 관리와의 상호작용, 암호화 파라메터, 암호화의 동기화, 암호화 알고리즘 등록 등이며, 디지탈 서명 관리(Digital Signature Management)는 키 관리와의 상호작용, 암호화 파라메터, 암호화 알고리즘, 개체간 사용 프로토콜 등의 관리이며, 접근 제어 관리(Access Control Management)는 패스워드 분배, ACL(Access Control List) 등이며, 키 관리(Key Management)는 키 생성 주기, 키 복사, 키 분배, 동작 키 교환 등이다. 데이타 무결성 관리(Data Integrity Management)는 키 관리와의 상호작용, 암호화 파라메터 및 암호화 알고리즘 설정, 사용 통신 프로토콜 등의 관리에 해당하며, 실체 인증 관리(Entity Authentication Management)는 패스워드, 키 분배, 인증 개체간의 사용 프로토콜 등의 관리 이다.

2.4 관리 보안 (Security of Management)

관리 보안은 관리 자체의 보안 관리로서 이는 관리 프로토콜 및 정보를 보호하기 위해서 적절한 보안 서비스 및 메카니즘을 선택하여 사용해야 하며, 관리 정보 자체의 통신 보안, 예를 들어 각 지역 노드의 MIB(Local Management Information Base) 개체간의 통신시 전송 정보의 보호와 전반적 관리 기능의 보안 유지, 보안에 관련된 MIB인 SMIB(Security Management Information Base)[20]의 안전한 유지가 이루어져야 한다. 이러한 관리 자체의 보안(Security of Management)의 표준화로 접근 제어 모델(Access Control Model : ISO/IEC 10164-9[18](또는 ITU-T X.741))과 접근 제어 정보 정의(Access Control Information Definition : ISO/IEC 10181-3(또는 ITU-T X.812))를 따라야 할 것이다.

2.5 일반적 보안 관리 사항

일반적인 보안 관리로 고려해야 할 요소[14]로는, 보안 관리 기능이 중앙 집중화되어야 바람직하다. 그 이유는 신뢰성 있는 부분이 최소화될 수 있으며, 보안 관리가 단순화될 수 있고, EDI 망의 전체에 일관성 있는 보안 정책의 적용이 용이하다는 점 때문이다. 따라서 일부의 보안 관리 기능은 중앙에만 존재가 가능해야 한다. 예로서 EDI 네트워크 침입 감지 기능은 침입 또는 오류 정보의 종합적 정보 수집과 분석을 통함으로써 감지 기능이 의미가 있으므로 관리의 중앙 집중화가 필요한 기능이다. 또한 추가적으로 고려해야 될 보안 관리 기능으로는 네트워크 개체 수정 시의 보안 문제보고, 재시험, 침입 발견시 해당 네트워크의 분리 운영이 필요하며, 사건에 대한 주기적인 보고, 즉 로그인 실패, 접근 실패, 근무 시간 외의 접근 등이 주기적으로 관리자에게 보고되어야 한다. 그리고, 기능의 예비 기능(백업 기능)을 위한 스위칭, 회복 서비스 등의 무결성 회복 기능과, 새로 생성 및 분배되는 암호화 키는 회복이 불필요하도록 해야 한다. 감사 분석(Audit Analysis)은 침입 감지와 달리 특정 보안 사건에 초점을 두며, 침입 감지는 감사 정보를 통합하여 분석하며, 감사 정보를 통계적 및 규칙 기반 방법 등으로 지적(Intelligent)으로 분

석한다. 따라서 이러한 침입 감지 기능은 안전한 시스템에 존재할 필요가 있다. 그 밖에 추가적 보안 관리 기능으로, 보안 자료의 시간에 따른 동기화(Synchronization) 및 백업으로, 보안 자료의 분배시 동기화 유지와 보안 정책의 일관성 유지가 필요하며, 중요한 회복 서비스로서 주기적인 백업과 백업 절차, 복구(Restore) 절차 정의가 필요하다. 추가적인 하드웨어, 소프트웨어의 설치 및 업그레이드 시 기본 패스워드, 계정의 간과에 주의해야 하며, 전반적인 망에 대한 보안 문제를 재분석, 재시험할 필요가 있으며 사용하던 자원의 재사용시 중요 정보가 존재하는지의 확인이 반드시 필요하다.

2.6 SMIB의 유지 관리

EDI 시스템과 관련된 모든 정보를 위한 개념적 보관 장소인 SMIB가 유지되어야 하며, 이 개념은 정보의 저장이나 이의 구현을 위해서 일정한 표준화 형식을 제시하지는 않는다. 그러나 각 종단 시스템(End System)은 적절한 보안 정책을 수행할 수 있도록 필요한 국지 정보(Local Information)를 포함해야만 한다. 이 SMIB는 종단 시스템을 물리적 혹은 논리적으로 그룹으로 묶어 일관성 있는 보안 정책을 수행할 수 있도록 확장된 분산된 정보 데이터 베이스이다. 실제 SMIB의 부분들은 중앙의 MIB와 통합될 수도 있고 그렇지 않을 수도 있다. 이 SMIB는 데이터의 테이블 형태, 파일의 형태, EDI 시스템의 하드웨어나 소프트웨어 내에 포함된 데이터나 혹은 규칙이 될 수 있다. 보안 관리 응용 프로그램에서 이 SMIB를 설정하거나 확장할 수 있어야 하며, 통신 프로토콜을 이용하여 수정할 수 있어야 한다. 따라서 적절한 보안 관리를 위하여 보안 관리자의 사전 승인이 필요하다. 국지적으로 유지하는 SMIB에는 예를 들어 암호화 알고리즘, 암호화 동작 모드, 암호화 키, 초기 벡터(Initial Vector), 파기 시간(Expiry Time), 보안 선택 인수(Security Selection Parameter), 서비스 가동(Activation), 서비스 중지(Deactivation) 등의 정보들이 유지되어야 하며, 저장된 정보들은 문맥(Context) 단위로 처리되며, 이를 보호 문맥(PRC: PRotected Context)라 하고 각각의 PRC ID(IDentification)에 의해 구분된다. 이러한 정보들은 각 호스트에 있는 국지 SMIB에 동일하게 저장되어야 하므로 EDI 시스템 보안 관리 프로토콜에 의하여 관리되어야 한다.

3. 보안 관리의 표준화

EDI 망 관리를 위한 기반 프로토콜 표준화는 OSI 기반 네트워크의 보안 보호(Security Protection)를 수용한다. 일반적인 망을 보호하기 위해 필요한 보안 기술들은 성숙되고 있으며, 제품에 실용화되고 있는 추세이다. 이 분야의 성숙으로 때로는 광범위한 보안 기술 가운데에서 어떤 기술 요소를 선택해야 하는가의 어려움에 봉착하게 되며, 보안 대책을 네트워크의 각 계층에 위치시킴에 있어서도 많은 선택들이 존재할 수 있다[2]. 일반적 네트워크 관리 프로토콜은 시스템, 네트워크, 네트워크 요소를 관리하기 위한 수단을 제공한다. 이 프로토콜은 구성 관리, 계정 관리 및 사건 로깅(Event Logging)과 같은 관리 기능들을 지원하며, 네트워크의 문제의 진단을 돕기 위한 편의를 제공해 준다. 네트워크 관리 프로토콜은 그 자체가 응용 프로토콜이며, 이 프로토콜은 다른 응용 프로그램과 같은 방법으로 하위 계층 통신 기능을 이용한다. 개방형 시스템 네트워크 관리 표준으로 OSI 관리를 위한 국제 표준에서는 CMIP(Common Management Information Protocol)를 정의하고 있다. 여기에서는 OSI 네트워크 관리 표준의 보안 측면을 다루고자 한다. 이 주제는 두 가지 서로 상이한 측면을 같이 다룬다.

- 보안 서비스 규정에 대한 네트워크 관리 프로토콜에 의한 지원(보안의 관리로 알려짐)
- 네트워크 관리 통신을 보호하기 위한 수단(관리의 보안으로 알려짐)

3.1. OSI 네트워크 관리 프레임워크

OSI 관리 표준은 ISO/IEC JTC1/SC21 소위원회에서 ITU와 공동으로 개발되었다. 이 표준은 CMIP 규격에 덧붙여 몇몇 네트워크 관리 프레임워크를 포함하고 있다. 그 개요를 살펴보면 다음과 같다. 첫 번째 OSI 관리 표준[4]은 1989년에 발간되었으며, OSI를 위한 관리 프레임워크를 정의(ISO/IEC 7498-4)[5]하고 있다. 여기에서는 2가지 형태의 관리를 구분하고 있는데, 하나는 OSI 시스템 관리로, 일반적인 시스템의 관리를 지원하고 있다. 다른 하나는 OSI 계층 관리로 특별한 OSI 계층 개체의 관리에 관계하고 있다. 관리 프레임워크는 5가지의 관리 기능별 영역인 구성 관리, 결함 관리, 계정 관리, 성능 관리 및 보안 관리를 정의하고 있다. 관리 프레임워크는 후에 시스템 관리 개요(ISO/IEC 10040)[9]에 의해 확장되었다. 이 표준은 OSI 관리 표준에 사용되는 용어를 정의하고, 기본적인 OSI 관리의 개념을 설명하며, 여러 가지 표준간의 관계를 기술하고, 이러한 표준에 관한 적합성을 위한 규칙을 설정하고 있다. OSI 관리 표준은 객체 지향 모델링 기법을 채용하고 있다. 관리될 대상 자원은 관리 대상 객체(managed object)로서 모델링된다. 관리 대상 객체는 그들이 받아들이는 행동과 그들이 내보내는 통보, 그들이 볼 수 있는 속성, 그들이 보여주는 행위에 의해 특징 지워진다. 실제의 네트워크에서 관리 대상 객체의 범주는 가상적으로 무한정이며, 관리 대상 객체의 정의는 다른 조직에 의해 만들어 질 수 있다. 관리 대상 객체는 봉쇄(Containment)에 근거하여 계층적으로 조정된다. 예로서, 하나의 파일은 여러 개의 레코드들을 포함할 수 있으며, 이 레크드들은 여러 개의 필드를 포함할 수 있다. 각 시스템을 위한 봉쇄 트리는 맨위(top)에 시스템 관리 대상 객체를 갖는다. 완전한 정보 모델은 관리 정보의 구조 표준(ISO/IEC 10165)[11]에 설명되어 있으며, 관리 정보 모델, 관리 정보의 정의, 관리 대상 객체의 정의를 위한 지침, 일반 관리 정보 등과 같은 여러 개의 부분들을 포함하고 있다. 더욱 발전된 표준으로서 ISO/IEC 10164[10]는 앞서 언급한 5가지 관리 기능별 영역에서의 여러 가지 관리 기능을 정의하고 있다. 한편, OSI의 구조적인 프레임워크는 관리하는 시스템과 관리되는 대상 시스템으로 구성되며 1개 이상의 관리 대상 객체를 포함한다. 두 시스템간에는 CMIP 응용 계층 프로토콜을 통하여 통신한다. CMIP는 ISO/IEC 9596[12]에 나타나 있다. CMIP에 의하여 제공되는 서비스는 CMIS(Common Management Information Service)로 알려져 있으며 ISO/IEC 9595[13]에 기술되어 있다. CMIP는 원격 운영 모델을 채용하고 있는 요청/응답 프로토콜이다. 그 서비스에는 2가지 형태가 제공된다.

- 관리 대상 객체에 의해 생성된 사건 통보의 전달(M-EVENT-REPORT 서비스)
- 관리하는 시스템에 의하여 호출되고, 관리 대상 객체에서 목표하는 동작의 전달

3.2 JTC1/SC21 WG4[2]에서의 OSI 관리

OSI 관리 표준은 보안의 관리(Management of Security)나 관리 보안(Security of Management)을 구별하여 언급하지는 않고 있다. 그러나, 그 표준들은 이 두 가지에 다 해당되는 요소들을 갖고 있다. "보안의 관리"를 지원하기 위하여 보안 경보 보고 기능, 보안 감사 추적 기능 등 2가지의 중요한 보안기능이 보안 관리 영역에서 정의되고 있다. "관리의 보안"을 지원하기 위하여 접근 제어 모델과 접근 제어 정보 정의 지원이 제공된다. 또한 규약이 CMIP 프로토콜에서 제한된 보안 기능을 위해서 만들어 진다. 한편, OSI 시스템 관리를 위한 ISO 프로젝트 10164에서는 다음과 같은 주요 보안 주제를 다루고 있다.

- DIS 10164-8 : 보안 감사 추적 기능(Security Audit Trail Function)[17]
- CD 10164-7 : 보안 경고 보고 기능(Security Alarm Reporting Function)[16]
- DIS 10164-9 : 접근 제어를 위한 객체 및 속성(Objects and Attributes for Access Control)[18]

3.2.1 보안 감사 추적 기능 (DIS 10164-8 : Security Audit Trail Function)

이 권고안은 보안 감사 추적 기능을 정의한다. 보안 감사 추적 기능은 중앙 집중형 또는 분산형 관리 환경에서 응용 프로세서에 의해 사용될 수 있는 시스템 관리 기능이며, 이 관리 환경에서는

시스템 관리를 목적으로 정보와 명령을 주고 받게 된다. 보안 감사 추적은 어떤 네트워크를 안전하게 함에 중요한 역할을 수행한다. 이 표준화 권고안에서는 다음과 같은 내용을 담고 있다.

■ 보안 감사 추적보고 기능을 지원하기 위해서 필요한 서비스 정의를 위한 사용자 요구사항을 설정
■ 보안 감사 추적보고 기능에 의해 제공되는 서비스를 정의
■ 그 서비스를 제공하기 위해 필요한 프로토콜 설정
■ 그 서비스와 관리 통보와의 관계를 정의
■ 적합성 요구사항(Conformance requirement) 설정

3.2.2 보안 경고보고 기능 (CD 10164-7 : Security Alarm Reporting Function)

이 권고안은 보안 경보보고 기능을 정의한다. 인증, 접근 제어, 비밀성, 무결성의 보안 서비스 모두에 발생될 보안 위협으로부터 보호할 목표를 갖고 있다. 그러나 이러한 서비스들은 항상 완전하게 제기능을 할 것으로 생각할 필요는 없다. 거기에는 적절치 못하거나 보호 메카니즘이 오동작 하거나, 예외적으로 교묘하거나 고질적인 공격 또는 메카니즘을 극복할 수 없는 환경(예로, 패스워드 분실 등) 때문에 항상 보안상 위험이 발생될 우려가 있다. 따라서 보안 위협이나 의심스러운 일이 발견될 때 이러한 사실들을 운영자나 관리자, 관리 책임자에게 보고를 할 필요가 있다. 이러한 보안 경보를 통해서 의심스러운 사용자에 대한 감시와 권한의 취소 또는 더욱 강한 보안 메카니즘을 호출하거나 결함이 발생한 네트워크 또는 시스템 요소를 수리하는 등의 후속 조치를 할 수 있게 해준다. 보안 경보는 원칙적으로 어떠한 네트워크이나 시스템 요소에 의해서 발견될 수 있는 보안 관련 사건에 의해 야기될 수 있다. 관리 모델에서는 사건을 발견하는 요소가 관리 대상 객체가 된다. 보안 경보는 M-EVENT- REPORT를 통해서 관리하는 시스템에 조언을 주게 된다. 보안 경보보고 기능 표준(ISO/IEC 10164-7)에서 M-EVENT-REPORT 호출시 전달되는 정보를 기술하고 있다. 교환시에 사용되는 축약 구문(Abstract Syntax)은 관리 대상 정보 정의(ISO/IEC 10165-2)[19]에서 기술하고 있다. 보안 경보 보고에서 전달되는 인수는 다음의 3가지의 범주로 나눌 수 있다.

■ M-EVENT-REPORT에 공통되는 인수는 ISO /IEC 9595에서 정의하고 있다 (즉, invoke identifier, mode, managed object class, managed object instance, event type, event time, current time).
■ 관리 정보에 공통되는 인수는 ISO/IEC 10164에서 정의하고 있다(즉, notification identifier, correlated notifications, additional information, additional text).
■ 보안 경보에 해당되는 인수(즉, 보안 경보 원인, 보안 경보 심각도, 보안 경보 발견자, 서비스 제공자).

이 표준안은 ISO 7498-4[5]에 의해 정의된 응용 계층에 위치하며, ISO/IEC 9594에 의해 제공되는 모델에 따라 정의된다. 시스템 관리 기능의 역할은 CCITT 권고안 X.700(ISO/IEC 10040)[9]에 기술되어 있다. 시스템 관리 기능에 의해 정의되는 보안 경보 통보(Security alarm notification)는 운영상의 조건, 서비스의 질, 보안에 관한 정보를 제공한다. 보안 관련 사건은 곧 보안 규약에 관계된 것이다. 보안 정책은 보안 관련 사건이 발생했을 때마다 취해야 할 행동을 결정하게 된다. 예로서, 보안 정책은 보안 관련 사건이 발생했을 때, 보안 경보 보고가 이루어지도록 하고, 보안 감사 추적에 사건 레코드가 만들어지며, 문턱 값을 증가시키고, 혹은 그 사건을 무시하거나 이러한 행위를 통해 적절한 조치를 취하도록 규정한다. 이 표준안은 보안 경보 보고에만 관련된다. 이 표준화 권고안에서는 다음과 같은 내용을 담고 있다.

■ 보안 감사 추적보고 기능을 지원하기 위해서 필요한 서비스 정의를 위한 사용자 요구사항을 설정
■ 보안 감사 추적보고 기능에 의해 제공되는 서비스를 정의
■ 그 서비스를 제공하기 위해 필요한 프로토콜 설정
■ 그 서비스와 관리 통보와의 관계 정의
■ 적합성(Conformance) 요구사항 설정

3.2.3 접근 제어를 위한 객체 및 속성 (DIS 10164-9 : Objects and attributes for access control)

이 표준화는 OSI 관리 서비스와 프로토콜을 사용하는 접근 제어 규약에 적용할 수 있는 규격이다. 이 규격은 다음과 같은 내용을 담고있다.

- OSI 관리 서비스와 프로토콜을 사용하는 접근 제어 규약을 위한 사용자 요구사항 설정
- OSI 관리 서비스와 프로토콜을 사용하는 관리 응용에 사용하기 위한 ISO/IEC 10181-3에서 정의한 전반적 접근 제어 모델의 해석 및 적용
- 접근 제어를 위한 절차 정의
- 시스템 관리를 위한 관리 대상 객체 클래스 및 속성 형태 정의
- 시스템 관리를 위한 접근 제어 정보의 교환에 필요한 프로토콜의 설정
- CMIP를 사용하는 관리에서 접근 제어 인수의 ASN(Abstract Syntax Notation) 규정
- 접근 제어를 지원하기 위한 인정 요구사항 규정

이 표준에서는 몇 가지 관리 대상 객체 클래스와 속성 형태 정의를 지원하고 있다. 이러한 정의는 ISO/IEC 10164-1[10]에서 정의된 절차를 이용하여 원격으로 접근제어가 다루어 질 수 있도록 할 수 있다.

3.2.4 CMIP 보안

CMIP(Common Management Information Protocol) 프로토콜 사양은 최소한의 보안 특성을 포함한다. 사실 내장된 보안 특성은 오직 관련된 동작 호출과 함께 접근제어 허가권(certificate)을 나르기 위한 규정뿐이다. 아무런 특정한 허가권 형식도 강제적은 아니다. 그러나 유럽의 ECMA 그룹의 작업에 근거한 가능한 허가권 정의는 ISO/IEC 10164-9[18]에 첨부되어 있다. 이것은 CMIP 통신이 보호될 수 없음을 의미할 필요는 없다. 그 이유는 보안에 대하여, OSI 모듈화 접근 방법은 다른 곳에 추가되어 보호될 수 있도록 하기 때문이다. CMIP 세션의 전체적 데이터 무결성 및 비밀성은 종단 시스템 수준의 보안 서비스를 이용하여 제공될 수 있다. 더 많은 종합적 응용계층의 보안 서비스는 일반적인 상위 계층 보안 기능을 이용하여 추가될 수 있다.

3.2.5 SNMPv2

1989년 TCP/IP에서 표준으로 채택된 네트워크 관리 프로토콜로 SNMP(Simple Network Management Protocol)는 프로토콜, 데이터 베이스 구조 및 데이터 객체 등을 포함한 네트워크 관리 프로토콜이며, 1993년에 데이터 인증(Data authentication), 무결성(Integrity), 비밀성(Confidentiality), 순차성(Sequencing) 등 4가지의 보안 서비스 기능이 추가되어 SNMPv2(Version 2)[7,8]로 향상되었다.

4. 보안 관리 도구

앞서 보았듯이 보안 관리는 네트워크 관리자로 하여금 호스트와 네트워크 자원에 대해 사용자 접근을 제한케함으로써 그리고, 보안 침투나 시도에 대해 그 관리자에게 보고케 함으로써 중요 정보를 보호하도록 할 수 있다. 네트워크 관리 시스템에서의 보안 관리는 소프트웨어 도구를 사용함으로써 실행된다. 이것이 어떻게 잘 수행되느냐는 관리자가 사용 가능한 도구의 기능에 달려 있다. 이 관련 도구는 단순, 복잡, 발전된 도구 등으로 구분하여 볼 수 있으며, 이 도구들은 네트워크 관리 시스템 상에서 보안 관리를 위하여 보안 대책이 어디에 존재하는가를 보여줄 수 있다. 그림 형태의 네트워크 지도에서의 입력에 따라, 이 도구는 사용자가 선택하는 어떠한 장치나 호스트에 적용 가능한 모든 보안 대책을 스크린에 보여줄 수 있다. 추가적으로 어떤 사용자나 네트워크 주소를 제한하도록 네트워크 내에서 모든 위치를 변경할 수 있도록 해 줄 수 있다. 그 도구는 구성 데이터 베이스(Configuration Database)에 질의(query)해서, 필요한 정보를 스크린에

보여준다. 이 보안 관리 도구는 이미 네트워크 관리 시스템에서 제공하는 구성 관리 정보를 사용하여, 네트워크에서 복잡한 연결 또는 접근 가능한 문제를 해결하는 게 매우 유용할 수 있다. 좀더 복잡한 도구는 중요 정보에 대한 접근점을 관찰하는 실시간 응용 프로그램을 갖도록 설계될 수 있다. 가능성 있는 보안 문제가 발생하는 즉시, 이 응용 프로그램은 그림으로된 네트워크 지도에 있는 영향을 받는 호스트나 네트워크 장비의 색깔을 변경시킬 수 있다. 또는 다른 사건들로 인해 색깔에 혼동이 생길 때는 관심을 끌도록 다른 방법으로 발견 사실을 보고할 수 있도록 하거나, 시스템 벨을 울리거나, 자동적으로 네트워크 관리 시스템 상에서 수행되는 윈도우에 발견 사실을 로깅하도록 설계할 수 있다. 또한, 발전된 보안 관리 도구는 복잡한 도구보다 더 개량되어, 보안 관련 사항에 관하여 사용자에게 안내하기 위해 모아 놓은 관련 교통 패턴 데이터를 사용한다. 더 완전한 보안 관리는 단순 도구와 복잡한 도구에서 언급한 기능 뿐만 아니라 이러한 기능도 필요로 한다. 개선된 도구는 사용자가 컴퓨터 혹은 장치에 설치코자 하는 보안 형태를 검사하여, 그 설치에 대한 가능한 반향으로 경고를 줄 것이다. 이 도구는 어떻게 보안 대책이 네트워크에 영향을 끼쳤는지를 분석하기 위하여, 역사 자료와 함께 사용자로부터 입력을 받아 사용할 것이다.

4.1 SMIB(Security Management Information Base)의 유지

EDI 시스템의 개념적 보안 정보 보관 장소로서 SMIB는 일반적으로 관계형 데이타 베이스 형태로 저장되며, 테이블 또는 파일 형태 또는 소프트웨어, 하드웨어에 포함이 가능하다. 이 SMIB는 네트워크의 종단 시스템 그룹별 분산 정보 베이스 형태로서 보안 정책 수행을 위한 지역 정보가 필수적으로 포함되어야 한다. EDI 네트워크의 전반적인 정보 데이터 베이스인 MIB와 보안에 관련된 정보 데이터 베이스인 SMIB는 통합되거나 또는 별도로 존재가 가능하며, 보안 관리 응용 프로그램에서 설정, 확장, 수정 가능이 가능해야 한다. 이의 사용시 보안 관리자의 승인이 필요하다. 시스템 보안 관리 프로토콜에 의해 호스트에 존재하는 SMIB와의 일치가 반드시 필요하다.

4.2 SMIB 관련 도구

SMIB(MIB)를 관리함에 있어 유용한 관련 도구로 MIB Compiler(RFC1155)가 있는데 네트워크의 지역의 각 장비로부터의 MIB 정보를 관리 시스템으로 적재해 주며, 그래픽 화면으로 MIB의 속성을 나타내 주는 기능을 수행한다. MIB Browser는 MIB 정보를 적재한 후 MIB 정보를 볼 수 있도록 해주며, MIB Query Tool은 네트워크 상의 각 장치들에 대하여 폴링하여 반환된 값으로 시험이 가능하다. 다음으로 MIB Alias tool(RFC1213)은 MIB 객체의 이름을 보안 관리자에게 친숙한 이름으로 바꿀 수 있도록 구성해 준다. 인터넷 상에서 관리 도구의 정보를 제공하는 사이트는 미국의 카네기 멜론 대학 OSLAB(CMU v2.1.2 SNMP)과 독일의 뮨헨 기술대학 WILMA[6] 팀(ftp://ftp.ldv.e-technik.tu-muenchen.de/dist/WILMA) 등이 있다.

5. 결 론

이제까지 EDI 망에서의 ITU-T X.800(또는 ISO/IEC 7498-2) 표준화에 기반을 둔 보안 영역 내에서 개발되고 있는 안전한 EDI 망에서의 보안 관리를 위한 요소를 다루었다. 아울러 최근의 표준화 활동, 소요 보안 기술, 네트워크 관리 통신을 보호하기 위한 표준화 요소 등을 알아보았다. 네트워크 관리를 위한 OSI 기반 프로토콜 표준화는 EDI 네트워크의 보안 보호를 지원할 수 있다. 네트워크 관리 프로토콜은 시스템, 네트워크, 네트워크 요소를 관리하기 위한 수단을 제공한다. 이 프로토콜은 구성 관리, 계정 관리 및 사건 로깅과 같은 관리 기능들을 지원하며,

네트워크의 문제의 진단을 돕기 위한 편의를 제공해 준다. 네트워크 보안 관리는 기술적, 관리적, 물리적 대책 등이 함께 인식되고, 구현될 때 비로소 그 조직의 중요 정보를 안전하게 유지 관리 할 수 있을 것이다. EDI 시스템의 보안 관리는 종합적으로 이루어져야 하며, 시스템 관리의 수작업과 자동화의 균형을 유지해야 한다. 왜냐하면 모든 관리 기능의 자동화에 따른 경비 문제, 관리자의 감시 및 판단의 문제가 발생하기 때문이다. 그리고, 관리를 위해서는 적절한 SMIB(MIB) 관련 도구의 활용이 바람직하다. 안전한 보안 관리는 난해한 문제로서, 계속적이고 종합적인 EDI 시스템의 보안 관리를 위한 포괄적 범위의 전체 보안 정책 유지, 관리가 종합적, 지속적으로 관리 유지될 필요가 있다.

참고문헌

[1] Allan Leinwand & Karen Fang, Network Management - a Practical Perspective, Addison - Wesley, 1993
[2] Warwick Ford, "Security Techniques for Network Management," IEEE, 1992
[3] Warwick Ford, Computer Communications Security : Principles, Standard Protocols and Techniques, Prentice Hall, 1994.
[4] ISO/IEC 7498-2, Information Processing System - Open Systems Interconnection - Basic Reference Model - Part 2 : Security Architecture, 1989.
[5] ISO/IEC 7498-4, Information Processing System - Open Systems Interconnection - Basic Reference Model - Part 4 : Management framework, 1989.
[6] R.Konopka & M.Trommer, 밃 Multilayer-Architecture for SNMP-Based, Distributed and Hierarchical Management of Local Area Networks, IEEE ICCCN?5, Sep.1995.
[7] B.Studer, Security Network Management, IEEE Infocom, 1994.
[8] William Stallings, Network and Internetwork Security, Principles & Practice, IEEE Press, 1995.
[9] ISO/IEC 10040: Information Technology - Open System Interconnection - System Management Overview (Also ITU-T Recommendation X.701)
[10] ISO/IEC 10164-1: Information Technology - Open System Interconnection - Systems Management: Object Management Function (Also ITU-T Recommendation X.730)
[11] ISO/IEC 10165-1: Information Technology - Open System Interconnection - Structure of Management Information: Management Information Model (Also ITU-T Recommendation X.720)
[12] ISO/IEC 9596: Information Technology - Open System Interconnection - Common Management Information Protocol Specification(Also ITU-T Recommendation X.711)
[13] ISO/IEC 9595: Information Technology - Open System Interconnection - Common Management Information Service Definition (Also ITU-T Recommendation X.710)
[14] John Kimmins, Network Security Management and Administration: Concepts and Issues, IEEE NOMS?2, 1992.
[15] ETRI, 정보보호 서비스 제공을 위한 안전성 서버 개발, 한국전자통신연구소, 1995.12.
[16] ISO/IEC 10164-7: Information Technology - Open System Interconnection - Systems Management: Security Alarm Reporting Function(Also ITU-T RecommendationX.736)
[17] ISO/IEC 10164-8: Information Technology - Open System Interconnection - Systems Management: Security Audit Trail Function (Also ITU-T Recommendation X.740)
[18] ISO/IEC 10164-9: Information Technology - Open System Interconnection - Systems Management: Object and Attributes for Access Control(Also ITU-T Recommendation X.741)
[19] ISO/IEC 10165-2: Information Technology - Open System Interconnection - Structure of Management Information: Definition of Management Information (Also ITU-T Recommendation X.721)
[20] ITU-T X.800, Data Communication Networks: Open Systems Interconnection(OSI): Security, Structure and Applications, 1991.