초고속 정보통신서비스용 보안 플랫폼의 요구분석

최락만•, 송영기, 김경범
한국전자통신연구소

Requirements on Security Platform for NII Services

Rakman Choe, Youngkee Song, Kyeongbeom Kim
Electronics and Telecommunications Research Institute

본 고는 초고속정보통신서비스의 안전성을 제공하기 위해 공통적으로 활용이 가능한 보안 플랫폼의 요구분석에 관한 내용으로, 먼저 초고속정보통신서비스의 환경에 존재하는 보안 위협과 대응 방안을 알아보고, 서비스 유형별로 요구되는 보안 특성을 살펴본 후, 보안 플랫폼의 요구사항을 일반적인 요구, 구조적인 요구, 기능적인 요구로 분류하여 제시한다.

1. 서론

앞으로 초고속정보통신망이 점차적으로 확대 구축됨에 따라 이를 이용한 응용서비스 또한 급격히 증가할 것이며, 이에 따라 개인의 은밀한 정보뿐 아니라 국가와 기업의 이익에 중대한 영향을 줄 수 있는 민감한 정보가 통신과정에서 누출될 가능성은 지금의 통신망에서는 느낄 수 없을 정도로 높아질 것이다. 이러한 상황에서 서비스 이용자는 그들의 정보가 송신될 때 불법적으로 수정되거나 폭로되지 않고, 원하는 수신자에게 전달될 것이라는 확실한 믿음이 있어야만 서비스를 사용할 것이다[1]. 이와 같은 보안문제는 초고속정보통신서비스를 실시하기 이전에 반듯이 해결되어야 할 과제이다.

본 고에서는 초고속정보통신망을 통해서 제공될 여러가지 유형의 정보통신서비스의 안전성을 제고하기 위한 보안 플랫폼(이하 "보안 플랫폼" 또는 "플랫폼"이라 함)의 요구사항을 제시하고자 한다. 이 플랫폼은 GSS-API(Generic Security Service API)와 같은 표준형 보안 인터페이스를 통해 인증, 접근제어, 데이타 기밀성(confidentiality)/무결성(integrity) 유지, 보안감사, 부인봉쇄 등과 같은 보안서비스를 쉽게 이용할 수 있는 환경을 제공해 주는 개방형 분산컴퓨팅 환경에 적합한 플랫폼이다. 이를 위해 우선 초고속정보통신서비스의 환경에 어떤 보안 위협과 취약점이 있는가 예측해 보고, 이러한 문제에 대처할 수 있는 일반론적인 대응 방안을 CORBA(Common Object Request Broker Architecture), SESAME(Secure European System for Applications in a Multi-vender Environment), POSIX, DCE(Distributed Computing Environment) 등에서 제공하는 기존의 보안 규격 및 서비스 등을 통해 알아본 후 초고속정보통신망을 사용하여 제공될 응용서비스의 유형별 보안 특성을 조사.분석하였다. 본 고는 이러한 조사/분석을 기반으로 보안 플랫폼의 요구사항을 일반적인 요구, 구조적 요구, 기능적인 요구로 분류하여 제시한 후 특정 응용에 실제로 적용할 때 고려해야 할 점과 향후 검토가 필요한 보안 관련 사항을 조명해 본다.

2. 초고속정보통신서비스 환경의 안전성 분석

초고속정보통신서비스의 환경은 인터넷, 공중교환망, 사설통신망, 유선/무선/위성 통신망 등이 유기적으로 연동되는 초고속정보통신망을 기반으로 하여, 지역적으로 분산된 이질적인 컴퓨팅 자원

을 엮어서 제공되는 여러가지 유형의 서비스를 다양한 사용자(일반 사용자, 서비스 제공업자, 정보 제공자 등)들에게 제공하는 개방형 분산컴퓨팅 환경이라 할 수 있다.

본 장에서는 초고속정보통신서비스의 환경을 보안이라는 관점에서 정보시스템 특히 개방형 분산컴퓨팅 환경에 어떠한 위협이 있고, 이러한 위협에 대응하는 방안을 살펴본 후, 서비스의 유형별로 요구되는 보안 특성에 대해 기술한다.

2.1 초고속정보통신서비스 환경의 보안위협와 대응방안

2.1.1 정보시스템에 대한 공통적인 보안 위협

사용자 관점에서 본 정보시스템 및 서비스에 대한 공통적인 보안위협들을 분류해 보면 아래와 같다.[1,6,7]

- 정보에 대한 불법적인 변조, 공개 행위
- 정보자원의 불법적인 이용
- 합법적인 서비스 요구에 대한 서비스 거부
- 정보의 발신 및 수신 사실에 대한 부인 행위 등

이러한 위협 요소들은 비인가된 사용자에 의해 발생하기도 하지만, 무책임하고 악의적인 인가된 사용자에 의해 발생할 수 있다. 아래와 같은 인가된 사용자로 부터 기인하는 위협은 예방하기 어려우나, 보안감사를 통해 인가된 사용자의 불법적인 행위를 저지하거나, 발생시 재빨리 복구할 수는 있다.

- 감사 또는 변경 통제절차를 거치지 않은 인가된 수정행위
- 간접적이고 임의적인 정보의 공개
- 합법적이지만 무책임한 자원의 사용 등

2.1.2 개방형 분산컴퓨팅 환경 고유의 보안 위협

개방형 분산컴퓨팅 환경은 일반적으로 구성요소들이 이기종으로 분산형태를 취하면서 계속 확장해가는 동적특성을 갖는다는 점 이외에도, 수많은 구성요소들간의 불명확한 신뢰관계, 다양한 보안정책의 상존, 상호작용의 복잡성, 분산된 다수의 관리자에 의한 보안관리 실행 등으로 일반적인 정보처리 환경에 비해 훨씬 더 보안에 취약하다. 개방형 분산컴퓨팅 환경의 특성으로 부터 오는 고유의 보안 위협들은 아래와 같다.[2,4,7]

- 부적절한 접근제어 및 공유공간의 재사용으로 부터 발생하는 인가된 사용자에 의한 정보누출
- 인가된 사용자를 가장한 시스템 이용
- 부적절한 권한 위임으로 발생하는 비인가된 정보접근
- 보안 통제 경로의 우회
- 통신선로 도청에 의한 비밀 정보의 획득
- 전송되는 정보에 대한 변조, 삽입, 삭제 등의 부당 행위
- 부적절한 사용자 식별로 부터 기인하는 책임 규명성 결여 등

2.1.3 보안 위협에 대한 대응 방안

상기 초고속정보통신서비스 환경의 보안 위협들에 대한 대응방안으로는 구성요소의 격리, 송신

정보의 암호화, 수신 정보의 검증, 서비스 통제, 운영기록 유지/분석, 탄력적인 시스템 구성 및 손상 복구조치 등이 있다.[1,2,4,6,7]

2.1.3.1 구성요소의 격리

모든 위협요소들에 대한 기본적인 대응방안으로는 보안이 필요한 모든 구성요소들을 보안영역으로 설정하여 외부와 격리시키고, 필요한 경우 그 보안영역이 미리 설정한 방법과 경로를 통하여 접근이 가능하도록 한다. 세부 방법으로는

o 안전한 환경 설정: 각종 시스템 구성요소 간에 불필요한 상호 간섭이 없도록 물리적/시간적/논리적인 방법으로 격리시켜 각종 보안 위협으로 안전한 환경을 제공한다.

o 자원 재사용에 의한 위협제거: 데이타 저장소와 같은 자원의 재사용으로 부터 기인하는 정보의 누출 문제를 예방하기 위해 사용이 끝난 데이타 저장소에는 잔류되는 정보가 없도록 정리한다. 이러한 조치는 응용서비스, 운영체제, 통신서비스 등 시스템을 구성하는 모든 서비스에 대해 취할 필요가 있다.

2.1.3.2 송신정보의 암호화

외부와 격리 조치가 취해지지 않은 통신선로나 데이타 저장소와 같이 보안성이 없는 일부 환경에 대해서는 아래와 같은 데이타 무결성 또는 기밀성 유지를 위한 별도의 보안조치를 취한다.

o 데이타 무결성 서비스: 송신측에서는 본문과 함께 암호화된 검사정보를 보내고, 수신측에서는 수신된 본문으로부터 수신자가 만든 방법과 동일한 방법으로 검사정보를 생성하고, 복호화된 수신 검사정보와 비교하므로서 정보의 무결성을 검증할 수 있다.

o 데이타 기밀성 서비스: 송신측에서는 정보의 노출을 방지하기 위하여 보내고자 하는 내용을 암호학적 메카니즘을 사용하여 암호화하거나, 정보 유추를 방지하기 위해 전송되는 정보에 트래픽 패딩(traffic padding) 처리를 하므로써 정보의 기밀성을 유지할 수 있다.

2.1.3.3 수신 정보의 검증

보안영역과 주체 또는 보안영역내 개체들은 서로 정보를 교환하므로서 상호작용한다. 보안영역에 대한 안전성은 아래와 같은 조치를 통하여 수신정보의 발신처 및 무결성을 검증하므로써 보안성을 유지할 수 있다.

o 정보 발신처에 대한 검증

- 접속기반형(connection-oriented) 서비스에서 정보 발신처에 대한 검증은 개체간에 상호작용이 일어나기 이전에 사용자 로그-온 또는 보안관계설정과 같은 식별 및 인증 프로토콜을 사용하여 제공될 수 있다.
- 전자우편과 같은 저장후전달(store and forward)형 서비스에서 교환되는 단위 메시지에 대한 발신처 검증은 전자 서명과 같은 정보발신처 인증메카니즘에 의해 제공될 수 있다. 이 경우에는 인증교환과 상호작용을 위한 정보교환은 동시에 이루어진다.

o 수신 정보의 무결성 검증

- 보안성이 있는 하드웨어, 운영체제, 네트워크서비스나 물리적으로 보안이 강화된 환경을

이용하므로써 정보교환의 무결성을 유지하는 방안.

- 개체간 통신에 검사정보 또는 전자서명 메카니즘을 명시적으로 이용하여 암호학적으로 무결성을 유지하는 방안

2.1.3.4 접근 통제

일반적으로 시스템 구성요소에서의 서비스 통제는 개체별로 부여되는 레이블 (label)과 같은 보안속성을 기반으로하며, 외부로 전달되는 권한속성과 자체적으로 보유하고 있는 제어속성을 이용하여 통제가 이루어지고, 이러한 보안속성은 보안 이외의 용도로도 사용될 수 있다. 시스템 구성요소의 유형별 서비스 접근통제 방식은 아래와 같다.

o 응용에 의한 통제 : 개별 응용들은 주체의 권한특성을 기반으로 하여 응용에 대한 특정 오퍼레이션 호출이나 데이타 엑세스에 대한 서비스 통제를 실시한다.

o 운영체제에서의 통제 : 운영체제는 통상적으로 프로세서에 대한 권한 검사를 통하여 운영체제의 특정 오퍼레이션 호출이나 데이타 엑세스에 대한 서비스 통제를 실시한다

.o 네트워크서비스에서의 통제 : 네트워크서비스에서는 출발점, 도착점 및 서비스 유형을 기반으로 각 노드에서 수발신 또는 중계되는 메시지에 대한 권한 검사를 통하여 서비스 통제를 실시한다.

2.1.3.5 운영기록 유지/분석

보안 관련 사건의 탐지와 증명은 책임규명성(accountability) 향상을 위한 조치의 하나이다. 이러한 조치는 예방적인 차원이기 보다는 더 이상의 피해가 발생하지 않도록 하는 억제조치라 할 수 있다.

o 사건 탐지 : 사건탐지는 수신정보 검증 및 서비스 통제 등에 문제가 발생할 경우에 대응하여 취할 수 있는 보안 관련 행위 중에서 기본적이고 능동적인 조치의 하나이다. 보안 관련 사건이 탐지되면 일반적으로 아래와 같은 조치가 취해진다.

  - 추후 분석이 가능하도록 사건 발생 내용을 기록
  - 보안 담당에게 경보를 전달
  - 유사한 사건의 재발방지를 위한 보안조치 강구 등.

o 보안 감사 : 보안감사는 보안 관련 사건 기록을 사후에 분석하는 행위로 보통 오프-라인(off-line) 형태로 이루어 진다. 보안감사는 발생한 사건의 유형을 파악하고, 보안 사고의 발생으로 부터 입은 피해를 파악하기 위한 일련의 사건을 추적하는 행위이다.

o 부인봉쇄 서비스 : 부인봉쇄는 사용자로 하여금 메시지의 수.발신 사실을 부인하는 행위를 방지하므로써 책임규명성을 제고하는데 그 목적이 있다. 부인봉쇄에서 사용하는 주요 기법은 아래와 같다.

  - 부인봉쇄에 사용될 정보를 신뢰할 만한 제3자가 수집, 제공
  - 암호학적 기법을 이용하여 부인 행위에 관련된 구체적인 사항의 수집 및 공증 처리

2.1.3.6 탄력적 시스템 구성 및 손상 복구조치

초고속정보통신서비스의 가용성을 제고하기 위해서는 다음과 같은 탄력적인 시스템 구성 및 손상

복구조치가 요구된다.

- o 특정 구성요소에 보안문제가 발생하는 것을 대비한 서비스의 이중화(redundancy).
- o 자원고갈로 인한 불법적인 서비스 위협에 대비하기 위해 일정한 양의 자원을 배정하는 방식채택
- o 연속해서 허용된 회수 이상의 인증절차를 통과하지 못하면 사용자 계정 또는 단말을 사용하지 못하도록 하는 방법

2.2 서비스 유형별 보안 관련 특성

앞으로 초고속정보통신망을 통하여 다양한 유형의 정보통신서비스가 제공될 것이다. 본 절에서는 이러한 서비스의 유형별로 요구되는 보안 특성에 대해 기술한다.[3,6,9]

2.2.1 오락, 소프트웨어, 컴퓨팅 서비스

디지탈 형식으로 전송이 가능한 오락, 소프트웨어, 컴퓨팅 서비스와 같은 지적재산은 쉽게 복사, 변경이 가능하다. 초고속정보통신망을 이용하여 이와같은 지적재산 유통서비스를 실시하기 위해서는 이들 지적재산권을 보호할 수 있는 기술적, 제도적 보호방안, 즉 합법적인 이용, 라이선스 및 사용료 지불 문제를 안전하게 처리하고, 불법적인 복사/변경/배포로부터 보호 및 음란물로 부터 미성년자 보호 등에 대한 방안이 강구되어야 한다.

2.2.2 의료, 교육 서비스

컴퓨터와 초고속정보통신망을 이용한 의료.복지서비스는 이 분야의 서비스 개선이라는 효과와 함께 개인정보의 불법적인 공개, 변조 및 이용이라는 부작용을 수반하게 될 것이다. 앞으로 초고속정보통신망을 통해 제공될 의료, 교육 서비스의 안전성을 위해서 아래와 같은 기술적인 사항이 검토되어야 한다.

- 의료, 교육정보의 무결성 유지
- 알 필요가 있는 사람과 시간에만 정보를 제공
- 정보를 용도에 따라 별도로 분리하여 관리
- 더 이상 효용이 없는 정보의 파기

2.2.3 금융, 보험, 상거래 서비스

신뢰성 문제로 수 십년간 폐쇠된 통신망을 이용하던 금융, 보험 산업 부문에서는 앞으로 금융망이 초고속 정보통신망으로 통합/연동되는 추세에 따라 금융 및 보험 정보의 기밀성과 무결성을 유지하기 위한 새로운 보안 기법과 조치를 필요로 한다. 상대방을 직접 만나지 않고서 이루어지는 금융, 보험 및 상거래에서는 상대방에 대한 신분 확인, 전자적 공증, 디지탈 서명, 날자 소인(date-stamping) 등이 매우 중요하다.

앞으로 많이 보급될 것으로 예상되는 전자화폐의 이용을 위해서는 전자화폐의 위조 및 소지자 인증 및 가명거래에 요구 문제를 어떻게 수용할 것인가에 대한 기술적인 대책이 마련되어야 한다. 또한 업체나 공공기관과 같은 조직의 정보를 개인의 불법적 이용으로 부터 보호하는 문제뿐 아니라, 앞으로는 개인 정보를 단체가 불법적으로 이용하는 것을 보호하는 방안이 마련되어야 한다.

2.2.4 지능형 운송 서비스

카메라나 전자 감지장치와 컴퓨터 칩이 내장된 카드를 이용하여 차량이 톨게이트에 정차하지 않고도 은행의 개인구좌와 연동시켜 통행료를 자동으로 징수하는 통행료자동처리 (electronic toll

collection)는 이외에도 교통상황 분석 및 운전자에게 최단 코스정보 제공 등에 이용이 가능한 지능형 운송서비스의 한 예이다. 이러한 서비스에서 통행료 처리에 따른 자금이체의 안전성 문제와 부가적으로 수집되는 차량소유주 정보, 주행속도, 목적지와 같은 정보는 개인의 영업정보 노출 및 개인 프라이버시의 침해를 초래할 수 있는 요인이 되므로 목적외에 사용되지 않도록 해야 한다.

2.2.5 공공정보 서비스

앞으로 인구센서스, 천재지변 대책, 사회복지 제공, 행정서비스 등 초고속정보통신망을 이용한 공공서비스가 실현되면 효율성있는 작은 정부의 구현이라는 긍정적인 효과와 함께, 국가정보의 무결성/기밀성/가용성 상실과 같은 보안 사고로 인한 국가와 국민에게 심각한 불이익 초래 가능성에 대비한 국가적인 대책이 요구된다. 앞으로 스마트 카드나 전자 직불카드는 후생복지와 같은 대민서비스에 많이 활용될 것으로 예상되는데, 이 경우 카드 분실, 위조 및 변조라든가, 전자카드의 사용으로 개인의 구매관련 정보의 노출과 같은 프라이버시 침해 문제가 발생할 가능성이 높다.

3. 보안 플랫폼의 요구사항

본 장에서는 앞 장에서 분석된 초고속정보통신서비스 환경의 보안위협과 대응방안을 기반으로 하여 정보통신서비스의 안전성을 제공하기 위해 공통적으로 활용이 가능한 보안 플랫폼의 요구사항을 제시하고자 한다. 보안 플랫폼의 요구사항은 성격에 따라 일반적 요구, 구조적인 요구, 기능적 요구로 분류할 수 있으며, 세부 요구사항은 아래와 같다[4,5,7,8,9].

3.1 일반 요구사항

3.1.1 일반성/범용성

플랫폼은 대다수의 사용자가, 다양한 응용 분야에서 , 여러가지 보안서비스를 제공하는데 사용할 수 있도록 일반성과 범용성을 갖어야 한다.

3.1.2 일관성(Consistency)

플랫폼은 기존의 정보처리 환경을 포함하는 개방형 분산컴퓨팅 환경하에서 보안 관련하여 아래와 같은 일관성을 지원하여야 한다.

- 이기종시스템을 포함하는 보안영역 내에서 보안정책에 의한 일관성있는 접근제어를 지원
- 기존의 접근제어 메카니즘 및 단-대-단 보안을 제공하는 환경을 수용
- 기존의 사용자 로그-온(logon) 방식을 무리없이 수용

3.1.3 사용의 용이성

플랫폼은 사용자, 보안관리자, 응용개발자 관점에서 아래와 같은 사용상의 용이성을 제공하여야 한다.

- 사용자는 단 한번의 로그-온으로 분산시스템내 모든 개체 및 서비스의 이용이 가능하여야 하며, 이해하기 쉽고 투명한 형식으로 보안서비스를 이용할 수 있도록 지원
- 보안관리자로 하여금 보안정책의 관리를 도메인 단위로 쉽게 할 수 있도록 지원
- 플랫폼은 보안이 전혀 고려되지 않은 응용에 대해서도 기본적인 보안서비스를 제공받을 수 있도록 하여야 하며, 특수한 보안조치를 필요로 하는 응용에 대해서는 응용 고유의 보안서비스를 쉽게 활용 가능하도록 지원

3.1.4 성능상의 요구

응용에 안전성을 제공하기 위한 보안기능의 추가로 인한 시스템 성능저하는 수용 가능한 범위 내에서 최소화되어야 한다.

3.1.5 보안 평가기준의 지원

플랫폼은 TCSEC(Trusted Computer System Evaluation Criteria)나 ITSEC(Information Technology Security Evaluation Criteria)과 같은 보안 평가기준에서 제시하는 보안 기능성 프로파일(Security Functionality Profiles)을 지원하여야 한다.

3.1.6 표준화

플랫폼은 현재 POSIX, OSF(Open Software Foundation), OMG(Object Management Group)에서 개방형 분산컴퓨팅 환경을 대상으로 추진하고 있는 표준 보안 프레임워크와 최대한의 호환성을 제공해야 한다.

3.1.7 보안 지침/규제에 대한 대책

플랫폼은 정부의 보안 메카니즘의 사용에 관한 관련 규정을 지원하여야 한다.

3.2. 구조적 요구사항

3.2.1 확장성

플랫폼은 소형뿐 아니라 대형시스템의 보안성 제공에도 응용이 가능하도록 아래와 같은 확장성을 제공하여야 한다.

- 접근제어는 사용자 개인별로도 가능해야 하지만 대형시스템의 관리적 부담을 줄이기 위해 사용자의 역할이나 소속그룹과 같은 권한속성을 이용하는 방법도 지원
- 서로 다른 보안 정책을 갖는 도메인 간에도 상호 연동이 가능토록 할 것
- 과도한 부담없이 대규모 네트워크에서 암호키를 안전하게 분배할 수 있는 수단을 지원

3.2.2 보안 통제의 강제성

플랫폼은 시스템에서 요구하는 기본적인 보안정책을 의무적으로 시행할 수 있어야 하며, 이러한 보안통제 경로를 우회하지 못하도록 해야 한다.

3.2.3 응용의 이식성

자체적인 보안이 필요없는 응용은 보안정책과 메카니즘이 상이한 환경으로 이식이 가능하여야 한다. 독자적인 보안을 필요로 하는 응용의 경우에 응용 고유의 보안정책은 시스템 보안정책과 일관성이 있어야 한다.

3.2.4 보안 정책의 융통성

기업에 따라 요구하는 보안정책은 다를 수 있으므로 필요로 하는 보안기능을 선택적으로 사용가능하여야 한다. 따라서 플랫폼은 기업마다 원하는 보안수준을 쉽게 설정할 있도록 하여 보안정책 채택에 융통성을 부여해야 한다.

3.2.5 보안 메카니즘과의 독립성

플랫폼은 응용의 필요에 따라 최적의 보안 메카니즘을 선택하여 사용할 수 있도록 보안 메카니즘으로 부터의 독립성을 가져야 한다. 이를 위해 플랫폼은 보안 인터페이스로서 GSS-API 와 같은 산업 표준을 지원해야 하며, 또한 여러 종류의 암호 알고리즘을 이용할 수 있도록 설계되어야 한다.

3.2.6 대치가능성

플랫폼을 구성하는 요소들은 응용의 성격, 기술의 발전에 따라 새로운 요소들로 쉬게 대치 가능한 구조를 가져야 한다.

3.2.7 상호 연동성

플랫폼은 아래와 같은 상호 연동성을 지원하여야 한다.

- 시스템 제공자가 다르고, 서로 다른 통신규약, 보안서비스를 갖는 이질적인 시스템간의 상호 연동성
- 동일한 분산시스템내에서 상이한 보안정책을 갖는 도메인간 상호 연동성
- 안정성이 전혀 없는 시스템과의 연동성

3.2.8 객체기술 지원

플랫폼은 향후 유지보수의 편이성 및 재사용성을 높이고, 기술적인 발전 추이를 고려하여 객체기술(Object-Oriented Technology)을 지원할 수 있어야 한다.

3.3 기능적 요구사항

3.3.1 식별 / 인증 서비스

사용자는 시스템을 이용하기 이전에 적절한 인증과정을 거쳐야 하며, 단 한번의 사용자 인증으로도 다수의 서버에 의해 제공되는 다종의 서비스를 이용 가능해야 한다. 사용자 인증은 필요에 따라 패스워드, 스마트카드, 신체특징인식 등과 같은 다양한 방식중에서 적합한 것을 선택적으로 사용할 수 있어야 한다. 또한 어떤 개체가 주체로서 역할을 할 경우 그 개체는 인증 과정을 거쳐야 한다. 인증을 거친 주체에게는 기본적으로 공인된 하나의 고유명과 함께 신임장(credential)이 부여되며, 필요에 따라서는 접근제어, 감사, 과금처리 등을 위한 별도의 고유명을 가질 수도 있어야 한다.

3.3.2 권한부여 / 접근제어 서비스

인증을 거친 주체는 시스템 사용 권한이 부여된다. 일반적으로 주체의 권한이 세분화 될수록 안전성은 높아진다. 따라서 플랫폼은 주체의 역할(roll), 소속그룹(group), 보안등급(security clearance)과 같은 다양한 권한속성을 기반으로 하는 접근제어를 지원하여야 하며, 주체의 권한 속성은 인가된 관리자 이외는 변경할 수 없어야 한다. 플랫폼은 다양한 보안 정책을 지원하기 위해 아래와 같은 여러가지 형태의 접근제어 방식을 수용할 수 있어야 한다.

- 누가 어떤 객체를 대상으로 무엇을 할수 있는가를 목록화하는 접근제어 목록 (Access Control Lists: ACLs) 방식
- 주체와 객체는 레이블(label) 형태의 보안속성이 부여되고, 어떤 주체가 특정 객체에 대해 어떤 행위를 할 수 있는가가 규정된 규칙(rules)에 의거하여 접근제어가 시행되는 레이블 방식
- 주체의 권한에 접근이 허용된 객체의 이름과 동작을 포함시키는 자격 (capability)기반 방식

3.3.3 데이타 기밀성 서비스

데이타 기밀성 서비스는 전송되는 메시지가 수동적인 공격으로부터 보호받도록 해 주는 기능이다. 가상 채널이 유지되는 동안 계속적으로 서비스하는 경우와 단위 메시지 혹은 메시지의 일부에 대해서만 비밀성을 제공할 수도 있다. 이러한 서비스에는 일반적으로 암호화 메카니즘이 사용된다.

3.3.4 데이타 무결성 서비스

데이타 무결성 서비스는 수신된 메시지가 중복, 삽입, 변조되지 않았으며, 재연(replay)된 것도 아니라는 것을 검증하는 서비스이다. 데이타 파괴의 경우에도 이 서비스가 적용대상이 된다.

3.3.5 보안감사 서비스

감사 기능은 사용자로 하여금 그들의 보안 관련 행위에 대해 책임을 지도록 하기 위한 기능이다. 사용자는 전체 응용 환경에서 인식될 수 있는 보안감사용 고유명을 가져야 하며, 감사용 고유명은 접근제어용과는 다를 수 있다. 또한 필요에 따라 익명을 사용 가능토록 하여야 한다. 플랫폼은 인증, 객체구동, 보안 관리 등 보안에 영향을 끼치는 중요한 사건들을 감사할 수 있어야 한다. 감사기록은 비인가된 사용자의 수정/삭제 행위로 부터 보호되어야 한다. 감사의 편의성을 위하여 감사 대상이 되는 사건들은 유형별로 분류되어, 필요에 따라 선택적으로 감사여부를 결정하고, 감사기록의 유지와 함께 보안 관리자에게 통보할 수도 있어야 한다. 감사기록의 분석을 위한 도구는 응용의 요구에 따라 제공될 수 있어야 한다.

3.3.6 부인봉쇄 서비스

플랫폼은 정보의 수.발신 행위에 대한 반박하기 어려운 증거를 제시하여 정보의 수신 및 발신 사실을 부인하는 행위를 저지할 수 있는 기능을 제공하여야 한다.

3.3.7 보안관리 서비스

플랫폼은 아래와 같이 보안정책을 설정하고 관리하는데 필요한 수단을 보안 관리자에게 제공하여야 한다.

- 보안영역의 설정과 관리
- 인증된 주체가 갖는 신임장의 기본 유효기간
- 객체간 통신시 기본 보호 수준
- 주체의 특권속성 및 객체의 제어속성 등 접근제어에 관련된 세부사항
- 주체의 권한 위임에서 위임의 범위, 내용, 조건에 관한 사항
- 감사 대상은 무엇이고, 감사에는 어떤 내용을 포함하여야 하는가에 대한 기준 등

또한, 관리 업무는 세분화(시스템관리,감사관리, 보안관리 등) 되어 여러명의 관리자에 의해 분담 관리될 수 있어야 하며, 영역별로 별도의 관리자에 의해 관리될 수 있어야 한다.

3.3.8 만국 표준시간 서비스

현재까지 안전한 시간소인(time stamping) 제공기법이나 시간서버는 개발되지 않았다. 기업간/업종간/국가간 교류가 빈번해 지고, 시간이라는 정보가 극히 중요한 역할을 하는 응용이 증가할수록 모든 사용자나 시스템이 공통으로 사용 가능한 만국 표준시각은 중요하게 된다. 따라서 플랫폼은 초고속정보통신망내 모든 사용자가 이용 가능한 만국 표준시간을 제공해 주어야 한다.

4. 결 론

초고속정보통신서비스의 환경은 기존의 정보시스템 및 서비스에 비해 더 많은 보안상의 취약요인을 안고 있다. 초고속정보통신서비스 사용자는 보안 문제로 인하여 자신에게 불이익이 발생하지 않는다는 확신이 없이는 서비스를 이용하지 않으려 할 것이다. 따라서 보안문제는 초고속정보통신

서비스를 실시하기 이전에 해결되어야 할 과제이다. 본 고에서는 이러한 해결 노력의 하나로 초고속정보통신서비스의 안정성 제공을 위해 공통적으로 활용할 수 있는 보안 플랫폼의 요구사항을 정립하였다.

본 고에서 제시된 보안 플랫폼의 요구사항은 총제적인 입장에서 초고속정보통신서비스의 보편적인 보안특성을 수용한다는 관점으로 도출되었기 때문에, 본 요구사항을 그대로 특정 응용분야에 대한 보안 요구사항으로 적용하는데 무리가 있다. 따라서 보안 플랫폼이 제시하는 요구사항 중에서 실제 응용에서 꼭 필요로 하는 보안 특성과 서비스만을 선택적으로 수용해야 하고, 보편성 문제로 플랫폼의 요구사항에 포함되지 않은 응용 고유의 요구사항은 추가되어야 한다. 또한 모든 보안 위협들에 대한 완벽한 보안조치는 현실적으로 불가능하며, 응용 대상에 따라 위협 요소들에 대한 요구되는 보호수준과 보호조치에 따른 소요경비, 성능 문제를 고려하여 균형있는 적절한 보안조치가 취해야 할 것이다.

한편으로, 향후 정보사회에서는 멀티미디어 중심의 정보통신서비스가 주류를 이룰 것으로 예측되기 때문에 멀티미디어 정보의 수용과 실시간 처리 요구증대에 따른 보안기능에 대한 검토가 필요하다. 또한 국익보호 차원에서 외국의 정보보호기술에 의존하지 않도록 독자적인 기술력 확보와 향후 전개될 초고속정보통신서비스에 이용이 가능한 보안 플랫폼의 조기 확보가 필요하다고 판단된다.

<참고 문헌>

[1] 정진욱, "초고속정보통신기반 구축에 따른 시스템 및 네트워크 시큐리티," 정보과학회지 제 14 권 제 3 호, pp.38 - 49, 1996. 3.

[2] 이영록, 노봉남,"CORBA 보안 구조," 통신정보보호학회지, 제 6 권 제 2 호, pp. 71 - 85, 1996. 6.

[3] 궁상환, 김성규,"초고속정보통신 기술개발 방향," 한국전자통신연구소 주간기술동향 94-47, pp.19 - 43, 1994.

[4] Object Management Group,"CORBA Security," OMG Document number 95-12-1, Dec. 1995.

[5] M. Neuman, "Security Consideration for NII," http://www.acl.lanl.gov/Sunrise/Security/ NSC_TOC.html, Jan. 1994

[6] "NII Security The Federal Role," IITF NII Securities Issues Forum, May. 1995

[7] IEEE,"Draft Guide to the POSIX Open System Environment: A Security Framework," Doc. number N013, p1003.22/D6, Aug. 1995.

[8] T. Parker, D. Pinkas,"SESAME V4 Overview," SESAME issue1, Dec. 1995.

[9] OSF, DCE Rel. 1.0 Internal Course - Student Guide Vol.2, Ver. Of April 15, 1992.