한국군사과학기술학회지 제12권 제5호, pp. 609~614, 2009년 10월

학술논문 정보기술 부문

일반망과 보안망을 연계한 네트워크 보안체계 설계

A Design for Network Security System via Non-security Common Network

조 창 봉* 이 상 국* 도 경 철*
Chang Bong Cho Sang Guk Lee Kyeong Cheol Dho

Abstract

In this paper, we have proposed a design for security network system passing through the non-security network which is commonly used for various networking services. Based on the security requirements which are assumed that the large classified data are bi-transmitted between a server and several terminals remotely located, some application methods of security techniques are suggested such as the network separation technique, the scale-down application technique of certification management system based on the PKI(Public Key Infrastructure), the double encryption application using the crypto-equipment and the asymmetric keys encryption algorithm, unrecoverable data deleting technique and system access control using USB device. It is expected that the application of this design technique for the security network causes to increase the efficiency of the existing network facilities and reduce the cost for developing and maintaining of new and traditional network security systems.

Keywords : Network Security System(네트워크 보안체계), PKI(공개키 기반 구조), Network Separation Technique(망 분리 기술), Asymmetric Keys Encryption Algorithm(비대칭키 암호화 알고리즘)

1. 서 론

정보통신기술의 발달로 네트워크 인프라에 대한 소요도 급속히 증가하고 있다. 인터넷 사용 초기에는 극히 제한된 용량의 자료 전송만 가능했지만, 최근에는 수 GB에 이르는 동영상을 비롯한 대용량 자료에 대한 전송 필요성도 제기되고 있으며, 이를 위한 네트워크 인프라의 확충과 관련 기술의 발달을 유도하고 있다[7]. 일반 가정에서도 100Mbps의 빠른 인터넷을 이용하는 것이 보편화 되었고, 이러한 인터넷 전송 속도를 기반으로 IPTV(Internet Protocol TV) 등의 고해상도 동영상 콘텐츠 제공 기술이 상용화 되었다. 네트워크 인프라는 개인의 생활 뿐 아니라 기업, 정부, 군 등에서 첨단 기술 및 응용 기술 개발을 위한 기술의 폭을 넓히는데 직접적인 영향을 주고 있다. 그러나 다양한 네트워크 전송 방식 및 자료의 종류와 목적에 부합하는 전송 소요를 모두 충족하기에는 아직 네트워크 인프라 자체가 충분하지 않으며, 특히 특정 목적으로 인터넷과 분리된 네트워크를 자체 구축하여 이용해야할 경우, 사용 빈도 및 사용자의 수에 무관하게, 전송하고자 하는 자료의 용량과 체계의 성격에 따라 막대한 구축비용과 운용유지 비용을 감수하면서 체계의 성능

† 2009년 5월 15일 접수~2009년 8월 31일 게재승인
* 국방과학연구소(ADD)
책임저자 : 조창봉(cbcho@add.re.kr)

을 유지한다[2].

국내 광역 네트워크 인프라의 대부분은 한국통신에서 구축하여 운용중이며, 사업자별 또는 군 체계별로 한국통신의 기간 네트워크의 일부 대역을 임차하는 방식으로 광역 네트워크 운용체계를 구축하여 사용하고 있다. 각 체계별로 구축하여 운용중인 개별 광역 네트워크는 공용 목적으로 사용하는 일반 네트워크에 비해 전송속도가 제한적이며, 광역 네트워크 이지만, 특정 사이트에 한정 구축되어 운용될 수밖에 없다. 일반 목적으로 공용 사용하는 네트워크 인프라를 중요자료의 전송에 이용하지 않는 가장 큰 이유는 보안 신뢰성이 확보되지 않았기 때문이다[4]. 최근 정보공유기술의 반대급부로 주요 정보 관리 체계에 대한 다양한 위협들이 급격히 증가하는 양상을 띠고 있으며, 국가별로 이에 대한 전문그룹을 양성하고 있는 상황이므로 정보보호에 대한 중요성은 그 어느 때 보다도 중요 항목으로 감안해야한다. 최근 Gap기술을 활용한 네트워크 게이트웨이를 이용하여 일반 네트워크와 체계 네트워크를 분리하면서 두 네트워크 간 자료교환이 가능한 기술이 개발되어 일부에서 운용되고 있지만, 보안 신뢰성의 확보가 충분하다고 할 수 없어, 중요 체계에는 단독으로 적용이 되고 있지 않다[6,8]. 자체 구축하여 운용중인 개별 네트워크 전송체계가 일반 네트워크 인프라를 이용할 경우, 막대한 비용절감 효과와 더불어 국가 기반 인프라의 활용성이 극대화 될 수 있을 것이다.

본 논문은 여러 체계가 공용으로 이용하는 일반 네트워크 인프라를 이용해 체계 서버와 원거리(광역 네트워크)에 위치한 소수 단말기 사이의 보호자료 전송이 가능한 네트워크 보안체계의 설계 개념을 제안하고 보안체계 설계시 고려해야하는 보안 항목 및 기능 구현을 위한 보안 기술 적용에 대해서 종합한다.

2. 네트워크 보안체계 설계

가. 보안체계 요구사항 분석

네트워크 보안체계를 설계하기 위해서는 보안체계가 보호해야할 자료의 성격에 대한 분석이 필요하다. 자료의 성격에 따라 우선시 되어야할 보안 요구 성능이 결정되며, 적용 보안 기술의 수준 및 구현 비용을 산출할 수 있다. 본 연구에서는 비도가 높은 대용량의 규정된 파일 자료를 기준으로 하며, 물리적/관리적 보안대책 수립시 요구사항은 논하지 않는다.

본 논문에서 네트워크 보안체계 요구사항을 다음과 같이 정의 한다.

- 체계 네트워크와 일반 네트워크의 물리적 분리
- 공개키 기반의 사용자 인증
- 전송 자료의 암/복호
- 임시저장 자료의 완전삭제
- 강제적 접근 통제

나. 체계적용 네트워크 보안체계 구성

1) 체계 네트워크와 일반 네트워크의 물리적 분리

네트워크 인프라가 우수한 일반 네트워크와 체계 서버 및 단말을 연계하기 위해서는 우선 체계와 일반 네트워크의 물리적 분리를 고려해야한다. 체계와 일반 네트워크를 직접 연결하는 것은 중요 정보를 불특정 다수에 노출시킬 위험이 있기 때문에 두 네트워크 간 물리적 분리는 필수 보안 요소라 하겠다. 따라서 두 네트워크 간 물리적 분리를 유지하면서 자료 교환의 편의성을 도모해야 함이 주요 연구 목표가 된다.

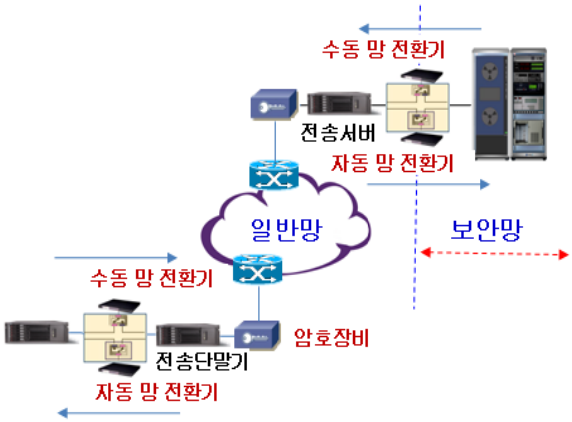


Fig. 1. 망전환 자료 교환기를 이용한 일반망과 보안망의 연동 구성도

일반망과 보안망의 연동을 위해 Fig. 1과 같이 수동 망전환기와 자동 망전환기를 혼용한 자료 전송 구조 및 절차를 제안한다. 일반적으로 TCP/IP 연결은 네트워크 각 서버에서 종료되므로 모든 프로토콜 계층의 세션이 끝나는 시점에서 끝나게 된다. 따라서 규정된 파일형태로 자료 전달하는 망전환 교환기를 가로질러 내부 서버까지의 직접적인 연결은 불가능하므로, 네트워크 수준의 취약점을 공격하는 프로토콜 기반의 공

격을 원천적으로 차단할 수 있다[7,9]. 자료 송신의 경우, 송신자가 자료의 송신을 인지하고 기계적으로 망전환기를 작동하여야만 보안망에서 일반망으로 자료의 전달이 가능하도록 하며, 송신자의 의지에 따라 송신된 자료는 일반망에서의 노출을 최소화하기 위해 자동 망전환기를 통해 자동으로 보안망의 단말기 및 서버에 전달 되도록 한다. 자동 망전환기는 스위치 제어모듈과 제어스위치, 자료스위치, 공유저장기로 구성되어 일반망에서 보안망 방향으로만 자료의 이동이 가능하며, 운용자의 개입 없이 시스템에 의해서 동작이 가능하도록 설계하여 적용한다. 보안체계 요구사항을 식별하기 위한 가정에서도 기술되었듯이 자동/수동 망전환기를 통해서는 기 규정된 파일 형태의 자료만 전달 가능하며, 명령이나 실행파일 등의 미식별 파일 및 메시지의 전달을 제한한다.

2) 공개키 기반(PKI) 사용자 인증체계

최근 공개키 기반의 비대칭키를 이용한 암호기술 및 사용자 인증서 관리기술이 보편화되어 인터넷 뱅킹이나 전자 상거래 등의 책임소재를 명확히 하여야 하는 사용자 인증체계에 적용되어 운용되고 있다.

그러나 국방인증관리체계(MPKI : Military Public Key Infrastructure)에서도 볼 수 있듯이, 공개키 기반의 인증관리체계 구축을 위해서는 인증기관(CA : Certification Authority), 등록기관(RA : Registration Authority)을 비롯하여 키관리 기관(KMA : Key Management Authority) 등의 조직과 개별 장비가 필요하다[5].

일반적인 대규모 인증관리체계를 소규모(50 사용자 이하)의 사용자 인증을 위해 구축하는 것은 경제적인 측면 뿐 아니라 운용인력에 대한 효율 측면에서 불합리하다. 그러므로 공개키 기반의 인증관리체계의 사용자 인증 기능 및 공개키 기반의 인증기술에서 응용되는 보안 기능을 사용할 수 있도록 소규모 체계 운용자를 위한 인증관리체계를 보완 개발하여 적용한다.

본 논문에서는 인증 및 등록 관리 조직은 전송서버의 실 운용조직에서 담당하고, 인증서버(CA)와 등록서버(RA)는 전송서버에 통합하여 설치 및 운용하는 Fig. 2의 개념을 제안한다. 이를 위해 인증서 발급 시 서버 운용자의 공개키를 함께 전송하여 인증서 피발급자가 소유할 수 있도록 하며, 발급된 인증서의 공개키는 서버운용자가 전자서명서 참조할 수 있도록 전송서버에서 관리한다.

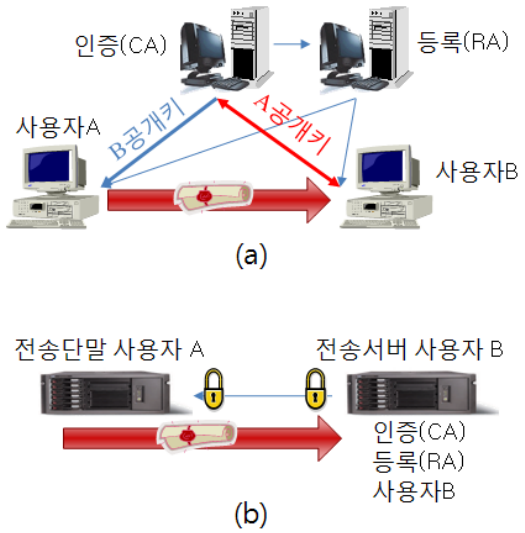


Fig. 2. 일반적인 인증관리체계 구성 및 운용방법(a)과 소규모 운용자를 위한 인증관리체계 구성 및 운용방법(b)

인증서버(CA)와 등록서버(RA)는 인증서 폐기목록을 관리하며, 갱신된 인증서 폐기 목록은 각 전송단말에서 발급받은 인증서 운용자에게 전송되어 참조되도록 한다. 전송단말에서 발급받은 인증서를 이용해 전자서명을 수행할 경우, 기 소유하고 있는 전송서버의 관리자의 공개키를 이용해 전송하고자 하는 자료를 암호화 하고, 송신자의 공개키를 전송자료에 포함해서 전송서버로 전송한다. 전송서버의 운용자가 전송단말의 운용자에게 자료를 전송할 경우, 기 소유한 수신자의 공개키로 전송자료를 암호화 하고, 송신자의 공개키를 전송자료에 포함하여 전송한다. 자료의 전송은 전송서버와 전송단말기 사이에서만 수행되므로, 서로 다른 전송단말기 운용자의 공개키를 각 단말기에서 소유할 필요는 없다. 기존의 검증된 CAPI(Crypto Application Platform Interface)의 호출 함수에 대한 변경 또는 추가 개발을 고려해야하며, 체계 적용을 위해 시스템 프로그램의 구현 절차와 기능을 세부적으로 설계하여 요구하는 성능에 최적화된 인증관리체계 적용이 가능하다.

공개키에 기반을 둔 인증관리체계를 적용함으로써 해쉬함수를 이용한 전송자료의 무결성 검증과 송·수신자의 확실한 인증을 통한 송·수신 부인방지, 운용이력에 대한 전자서명을 통해 이력의 위·변조 방지 기능 등의 구현 적용이 가능하다.

3) 전송자료의 암 · 복호

네트워크를 이용한 자료 전송에 관한 보안 기술 중 가장 중요한 보안설계 고려항목이 자료의 암 · 복호화 기술이다. 전송자료의 암 · 복호화 기술의 완성도는 정상적인 절차를 거치지 않고 암호화된 자료를 복호하는데 소요되는 시간으로 결정될 만큼 완벽한 암호화란 존재하기 어렵다. 특히 일반망을 경유하는 보안체계를 설계할 경우, 불특정 다수에게 공개되는 자료의 보호를 위해 검증된 암호기술 및 암호장비에 의한 암호화가 필수적이다.

가) 암호장비

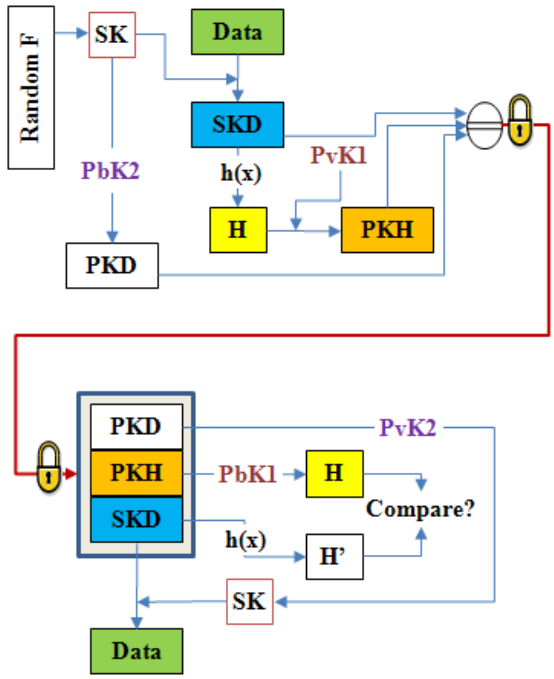
암호장비를 이용한 암호화의 경우, 전송자료가 평문상태로 존재하는 네트워크 구간을 최소화해야한다. Fig. 1에서 전송서버와 전송단말기가 일반망에 연결되는 바로 앞단에 암호장비를 설치하도록 네트워크 보안체계를 설계하는 이유이다. 현제 운용중인 암호장비의 대부분은 1:1 암호장비이다. 1:1 암호장비는 전송단말기와 전송서버사이의 암호터널을 형성하기 위해 2개의 동급 암호장비를 설치하여 운용하는 것이다. 1:1 암호장비의 경우 전송서버 단에 전송단말기의 수만큼 암호장비를 설치/유지하여야하는 단점이 있다. 최근 1:N 개념의 다중 접속이 가능한 암호장비가 개발되어 신규 체계에 적용되고 있다.

암호장비를 이용한 전송 성능은 암호장비에서 전송대상 자료를 암호화 또는 복호화 하는데 소요되는 시간으로 결정된다. 특히 1:N 개념의 암호장비의 경우, 암 · 복호 속도가 네트워크 체계 성능을 좌우할 수 있다. 일반망에 보호자료를 유통하기 위해서는 암호알고리즘 및 암호화 기술이 공개되지 않은 검증된 암호장비임과 동시에 1:N 접속이 가능하며 네트워크 전송속도에 지장을 주지 않는 암호장비를 적용한다.

암호장비를 필요로 하는 체계의 기대 기능이 지속적으로 고도화 되고 있고, 이에 맞추어 다양한 기능을 갖춘 고성능의 암호장비가 지속적으로 개발되고 있으므로, 보안체계 설계시 암호장비의 개발추세 및 개발중 암호장비의 개발완료 시점 등을 고려하여 보안체계의 성능 향상시킬 수 있도록 한다.

나) 비대칭키를 이용한 암호화

일반망을 이용한 보호자료의 전송을 위한 보안체계 구축을 위해서, 암호장비를 이용한 하드웨어적 암호화와 별개로 공개키 기반의 소프트웨어적인 암호화를 적용하여 2중 암호화를 구현하는 것이 바람직하다. 본 논문에서 제안한 공개키 기반의 사용자 인증체계를 적용함으로 해서 별도의 비대칭 암호기술 적용 없이 구현 가능하다.



PbK1 : 송신자의 공개키, PbK2 : 수신자의 공개키
PvK1: 송신자의 개인키, PvK2: 송신자의 개인키
h(x) : 해쉬함수, H :해쉬값
Random F : 렌덤함수
PKD : 공개키로 암호화한 자료
PKH : 공개키로 암호화한 해쉬값
SKD : 대칭키로 암호화한 자료, SK : 대칭키

Fig. 3. 공개키 기반의 비대칭키와 대칭키의 혼용 암 · 복호과정 및 암호장비를 이용한 2중 암 · 복호의 기능 구성

일반적으로 자료를 암호화하기 위해서 일정한 크기의 키(Key)값을 사용한다. 키 값의 크기(bit 수)에 따라 암 · 복호의 성능 및 기술 수준을 가늠하기도 한다. 자료를 암 · 복호화하기 위해서 적용한 키 값의 동일 여부에 따라서 대칭키 암호기법과 비대칭키 암호기법으로 구분한다. 비대칭키를 이용한 암호기술은 수신자의 공개키로 전송 파일을 암호화 하고 수신자의 개인키로만 복호가 가능한 기술이다[3]. 일반적으로 대칭키에

의한 암호화 기술보다 보안성은 우수하나 암·복호시 시간이 오래 걸린다는 단점이 있다. 그러므로 암·복호 시간이 빠른 1회성 대칭키를 렌덤함수를 통해 생성하고, 임시로 생성된 대칭키를 이용해 보호자료를 암호화 한다. 자료 암호화에 이용된 대칭키를 수신자의 공개키로 암호화하여 전송하는 기법을 적용하면, 비대칭키 암호화 기법의 보안성을 유지하면서 대칭키에 의한 암호화 단점인 암·복호 속도 저하 문제를 보완할 수 있다(Fig. 3).

수신자의 공개키를 이용해 대칭키를 암호화하면 수신자의 개인키를 이용해야만 복호화가 가능하므로 전송자료의 수신부인방지 기능을 구현할 수 있으며, 전송자료의 해쉬값에 대해 송신자의 개인키로 암호화하면 송신자의 개인키에 의해서만 복호가 가능하므로 송신부인방지의 근거가 된다. 송신자의 개인키로 암호화한 해쉬값은 전송된 자료와 동일한 해쉬함수를 통해 계산할 수 있으며, 수신자가 계산한 해쉬값과 비교하여, 전송된 자료의 위·변조 여부를 확인한다.

공개키와 대칭키의 혼용에 의한 비대칭키 자료 암호와 별개로, 전송이 수행되는 전송서버와 전송단말기의 양 끝단에 설치된 암호장비는 암호터널이 형성되는 양끝에서 전송되는 모든 자료를 상이한 알고리즘의 암호방식으로 암호화하므로 2중 암호화에 의한 자료 보호가 가능하다.

4) 임시저장자료의 자동 완전삭제

일반망을 이용해 전송되는 자료는 암호장비 및 암호기술, 접근통제 기술에 의해 보호되지만, 일반망에 노출되는 시간을 최소화 하여야한다. 또한 전송을 위해 일시적으로 일반망에 물리적으로 연결된 장비에 기록되었던 자료는 전송완료 확인 후 완전삭제를 수행하여 복구가 불가능하도록 설계한다. 일반적인 완전삭제 프로그램은 운용자에 의해 삭제된 자료를 지정된 보조기억매체의 물리적 주소에 이동하여 모아 놓고, 운용자의 의지에 의하여 완전삭제 기능을 수행한다. 자료의 전송이 완료된 후의 임시저장자료에 대해서는 운용자의 추가 개입 없이 자동으로 완전삭제 되도록 구현하는 것이 바람직하다. 자동 완전삭제 대상에는 복호된 자료와 복호되기 전의 암호화된 자료를 포함한다.

완전삭제 기능은 자료가 저장되었던 보조기억매체의 물리적 위치에 난수로 구성된 문자를 지정된 회수만큼 덮어쓰기를 하는 것으로 구현한다. 일반적인 완전삭제 방식은 Gutmann, US DoD 5220-22.M, Pseudorandom (ISSAAC 알고리즘) 기법 등이 있으며, 마그네틱 디스크의 하드웨어적인 복구로부터 안전을 보장하기 위해서는 35회 덮어쓰기를 권장한다. 전송 및 수신 후 전달이 완료된 자료는 1회의 덮어쓰기를 수행한 후 임의 저장 폴더로 이동된다. 임시저장 폴더에 이동된 삭제자료는 해당 장비의 시스템 부하가 적은 상태를 점검하여 지정된 회수만큼 덮어쓰기를 수행한다. 시스템의 부하 점검에 의한 자동 완전삭제 뿐 아니라, 임시저장 폴더에 저장되어 있는 자료를 운용자의 의지에 의해서 우선적으로 완전삭제 수행이 가능하도록 설계한다(Fig. 4). 기본적으로 덮어쓰기 회수를 35회로 설정해 놓으며, 삭제 자료의 종류와 운용편의에 따라 1, 3, 7회로 변경 가능하도록 설계한다.

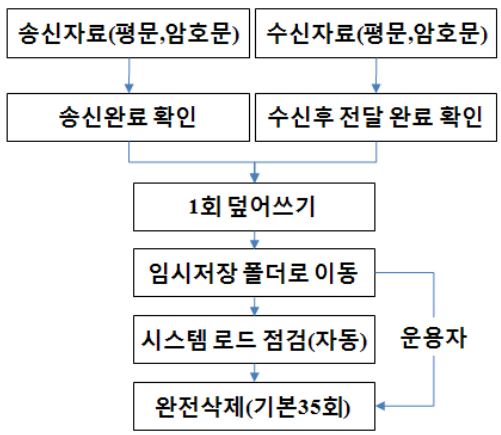


Fig. 4. 전송을 위해 임시 저장된 자료의 완전삭제 기능 구현 흐름

5) 강제적 접근통제

공개키 기반의 사용자 인증관리체계를 적용하여 인증서 소유 여부를 확인해, 보호장비의 운용권한을 부여하는 방식으로 보호장비에 대한 접근을 통제할 수 있다. 또한 지문인식이나 홍채인식 등의 사용자 인증기술을 적용하여, 중요 시스템 접근시 생체인식을 통한 접근 통제를 구현하고 있으나[1], 시스템의 운용체계가 구동되기 전에 보호장비 운용 권한을 부여할 수 있는 강제적 접근통제기술의 적용 또한 필요하다.

강제적 접근통제를 위해 스마트카드 및 카드 인식기를 시스템에 장착하여 운용하는 방법이 있으나, 최근에는 USB 형태의 강제적 접근제어 및 공개키 기반의 인증서를 탑재하여 사용자 인증에 의한 접근제어 및 자료 암·복호도 가능한 장비가 개발되어 운용중이

다. 카드 인식기 등의 별도의 장치가 불필요하고, 일반적인 전산장비에서 제공하는 USB 포트에 연결하여 운용 가능하므로 개발 및 운용이 용이하다. 일반망을 경유하는 보안체계임을 감안하면, 기계적 장치를 이용한 강제적 접근통제 기능의 적용이 요구됨으로 설계에 반영한다.

3. 결 론

국내의 현재 네트워크 인프라 상황에서, 일반망과 보안망을 연계한 보안체계를 구축하여 운용함으로써 기대할 수 있는 효과는 막대한 경제적 이익 뿐 아니라, 네트워크 기반 부족으로 미개발된 중요 체계 구축 시기를 앞당기고, 관련 기술 발전 및 소요 체계의 조기 전력화에 기여할 수 있을 것으로 예상된다. 일반적으로 보안성과 운용 편리성은 상치된 개념으로 받아들여지고 있다. 보안체계 설계에 있어서 보안 신뢰성 확보가 어느 항목보다도 우선해야함이 명확하지만, 운용 편리성을 고려하지 않은 시스템은 운용자의 불만을 초래하기도 한다. 구축하고자 하는 보안체계의 요구 성능을 명확히 분석하여, 요구되는 성능을 운용 편리성을 고려하면서 구현 가능하도록 보안체계를 설계하며, 망의 물리적 분리 기술의 적용 방법, 사용자 인증 관리 기술, 송 · 수신 자료의 보호, 송 · 수신 부인방지, 자료의 무결성 확인 등의 보안기술에 대한 적용 및 운용 지침을 수립하여 보안체계 설계에 반영될 수 있도록 한다.

본 논문에서는 원격지에 위치한 체계의 서버와 단말기 사이의 자료 전송을 위해 일반망을 경유하는 네트워크 보안체계 설계 방안을 제안하였다. 체계의 구축 목적과 전송 단말간의 위치와 개수 및 전송할 자료의 성격에 따라 적절한 보안체계 설계가 이루어져야 할 것으로 사료된다.

Reference

[1] 김이형, “생체/지문인식 기술동향 보고서”, 국방과학연구소, IEDC-509-010845, 2001.

[2] 문은점, 도경철, 조창봉, “다중매체 DB 보안시스템 구축 개념 연구”, 국방과학연구소, NSDC-514-041387, 2004.

[3] 박영호, “정보보안을 위한 암호학-공개키 암호”, 물리학과 첨단기술, pp. 7～12, 2007.

[4] 양대일, “정보 보안 개론”, 한빛미디어, 2009.

[5] 양상운, 김영진, 박중길, “군 PKI 구축 방안에 관한 연구”, 통신/전자 학술대회 논문집, pp. 227～283, 1998.

[6] 이윤경, 박찬호, 권영찬, 강수현, 윤호상, 장희진, 김철호, “Gap기술을 활용한 보안 네트워크 게이트웨이 구성에 관한 연구”, 통신/전자 학술대회 논문집, pp. 65～69, 2007.

[7] 임철수, TCP/IP 인터넷트워킹, 도서출판 그린, 2003.

[8] Kevin Gennuso, Disconnect from the Internet-Whale's e-Gap In-Depth, SANS Institute InfoSec Reading Room, Sep. 13, 2001.

[9] Michael Bobbtt, “(UN)BRIDGING THE GAP”, http://infosecuritymag.techtarget.com/articles/july00/cover.shtml