通信情報保護學會誌
第 11 券 第 1 號, 2001. 2

초고속국가망 가입자 정보보호 방안

한 치 문*, 이 형 옥**

Ⅰ. 서 론

최근 인터넷의 확산으로 인터넷을 이용한 업무가 날로 증가하고 있으며, 이를 뒷받침하기 위한 정보통신의 인프라에 대해서도 많은 연구가 진행되고 있다. 우리나라에서도 초고속국가망을 구축하여 정보통신의 네트워크 하부구조로서 역할을 충실히 이행하고 있다. 그러나 초고속 인터넷 서비스 수요의 증가만큼 정보를 이용하는 생활의 변화가 동반하지만, 그의 역기능 또한 증가하고 있다. 예를 들면 정보의 노출로 인한 개인 사생활의 침해나 경제적인 손실 등을 말 할 수 있다.

정보의 노출은 본인의 실수나 해커에 의해 발생하므로, 이러한 문제를 궁극적으로 차단 할 수 있는 보안 기술이 오늘날 중요한 문제로 부각하고 있다. 앞으로 보다 윤택한 정보화 사회에 진입하려면, 먼저 정보보안에 대해 많은 노력을 기울이지 않으면 안될 것이다.

따라서 현재 운용하고 있는 초고속국가망은 전국적으로 28,000여 개의 공공기관이 접속되어 있으므로, 각 기관이 갖고 있는 데이터나 정보 흐름에 대해서는 완벽하게 해커로부터 보호해 주어야만 된다. 즉 초고속국가망에 접속된 가입자에게 초고속국가망 보안에 대해서 신뢰감을 주어야 한다. 그러기 위해서 사전에 초고속국가망의 보안 취약점을 분석하여, 대응 방안을 체계적으로 연구해 둘 필요가 있다.

본 고에서는 초고속국가망에서 가입자 정보보호 방안을 검토하고자 한다. 서론에 이어 제2장에서는 초고속국가망의 가입자 유형을 가입자 네트워크 토폴로지 관점에 따라 프레임릴레이 가입자망과 사설 ATM 가입자망 그리고 라우터 가입자망으로 구분한다. 또 가입자 네트워크의 사용 기능에 따라 인터넷 백본 모델, End-Sit간의 전용선 기능의 Virtual Tunneling 모델, VPN 이용 모델로 분류하였다. 제3에서는 사용 기능별로 분류한 3개의 유형을 네트워크 토폴로지에 따라 3가지 형태로 분류하여, 각 유형에 따른 가입자 정보보호 방안을 설명한다. 제4장에서 사업자가 구축하는 초고속국가망에 대한 보안 방법을 간략히 제시하고, 제5장에서 결론을 맺는다.

Ⅱ. 초고속국가망 가입자 유형 분석

초고속국가망은 ATM를 기반으로 하는 백본 네트워크로 여러 유형의 가입자를 접속하여 IP 기반의 데이터 서비스를 제공하고 있다. 현재 초고속국가망에서 IP 제공방식은 IP over ATM(Classical IP over ATM) 기술을 이용하고 있지만, 향후 MPLS 기능을 제공할 계획이다. 다른 특징은 PVC 형태로 구성하여 가입자 네트워크에 터널링 기능을 제공하고 있다.

초고속국가망에 수용되는 가입자를 유형별로 분석하면, 네트워크 토폴로지에 따라 구분하는 방법과 초고속국가망 사용 기능에 따라 구분하는 방법으로 생각 할 수 있다. 이를 바탕으로 초고속국가망의 보안 모델을 사용자 유형별로 정립 한다. 먼저 가입자가 소속되어있는 네트워크 토폴로지에 따라 구분하면 다음과 같은 유형으로 나눌 수 있다.

1. 네트워크 토폴로지에 따라 분류

1.1 프레임릴레이(Frame Relay) 망에 접속된 가입자

프레임릴레이 교환기를 사용하여 사설망을 구성

* 한국외국어대학교 전자정보공학부
** 한국전산원 국가정보화센터

및 운용하는 가입자가 초고속국가망에 접속하는 방법으로 E1급일 때는 ATM 교환기의 프레임릴레이 모듈에 접속되며, 64Kbit/sec 급일 때는 가입자 정합장치를 통하여 접속하는 구조를 갖고 있다. 이때 FR(Frame Relay) NNI 기반의 초고속국가망 접속 인터페이스를 갖는 경우는 정합장치 이용하여 접속한다. ATM UNI 기반의 초고속국가망 접속 인터페이스를 갖는 경우 접속속도가 STM1급이면 교환기에 직접 접속하고, E1급이면 교환기에 직접 접속 또는 정합장치 이용하여 접속하고 있다. 한편 다른 유형의 가입자 네트워크의 단말과 통신하기 위해 서비스 연동 기능을 ATM 교환기 또는 정합장치에 구현하고 있다

1.2 사설 ATM 네트워크에 접속된 가입자

ATM 교환기를 사용하여 사설망을 구성한 가입자가 초고속국가망에 수용되는 경우이다. 이때 DS3급 이상인 경우는 ATM 교환기에 직접 접속하고, E1급인 경우는 가입자 정합장치를 통하여 ATM 교환기에 수용되고 있다. 그리고 IP 단말의 경우는 ATM망에서 사용하고 있는 IPOA 기능을 이용하고, ATM 단말인 경우는 네트워크상의 변환 기능이 필요 없이 초고속국가망에 접속된 다양한 서버를 이용할 수 있도록 구성하고 있다. 또 ATM망에서 사설 ATM 망간의 SVC 정보 전송기능이 필요하므로 Virtual Tunneling 기능을 제공하고 있다

1.3 라우터망에 접속된 가입자

라우터를 사용하여 사설망을 구성한 가입자를 초고속국가망에 수용하는 경우이다. 이때, FR(Frame Relay)로 접속하는 E1 라우터 가입자는 프레임 릴레이 교환기를 통하여 수용되고, 64Kbps 라우터 가입자는 정합장치를 통하여 ATM 교환기에 수용되고 있다. 라우터가 45Mbps, 155Mbps로 ATM 인터페이스를 갖는 경우는 ATM 교환기에 직접 접속된다. E1 속도의 접속 가입자는 가입자 정합장치를 통하여 ATM 교환기에 수용하고 있다. 또한 FR 라우터로 초고속국가망에 접속하는 경우는 FR망에 접속된 가입자와 동일한 방법으로 접속 기능을 제공하고 있다.

라우터가 ATM 정합장치를 갖는 경우는 직접 물리적으로 접속된 후, IPOA (RFC1577)를 사용하여 ATM망 서버에 접속된다. 이때 라우터 가입자간의 트렁크 역할을 ATM 네트워크가 제공하도록 가입자 라우터와 ATM 네트워크 사이에 Network Interworking 기능을 구현하고 있다. ATM 인터페이스를 갖는 라우터를 이용하여 초고속국가망에 접속하는 경우는 ATM PVC 또는 SVC를 이용하고 있다. 현재는 PVC 방식을 사용하고 있다.

1.4 기타 가입자

LAN 환경 및 라우터에 접속된 가입자가 ATM 정합장치와 프레임릴레이 정합장치로 접속하는 경우가 있다. 각각은 라우터에 접속된 가입자와 동일한 방법으로 수용한다. 초고속국가망에서 가입자는 기관 가입자가 대부분이지만, 불특정 일반 가입자 수용을 고려하여 초고속공중망 사업과 연계하여 검토하고 있다.

이상은 초고속국가망 가입자를 초고속국가망에 접속하기 위해, 가입자가 소속된 네트워크 토폴로지에 따라 분류한 것이다.

2. 초고속국가망 사용 기능에 따라 분류

초고속국가망 가입자가 초고속국가망에 접속되어 서비스되고 있는 기능별로 분류하면, 대체적으로 다음과 같다.

① 인터넷 백본 모델
② End Site간에 전용선 기능의 Virtual Tunneling 모델
③ VPN 모델 등

초고속국가망에 접속되는 가입자는 상기 3가지 기능 중 하나를 이용하고 있다. 대부분 가입자는 End Site간에 전용선 기능의 Virtual Tunneling 기능을 이용하며, 이때 회선 설정은 PVC 방법을 적용하고 있다. 또 인터넷의 백본으로도 이용하고 있다.

초고속국가망의 가입자 네트워크 토폴로지에 따라 구분한 것을 요약하여 나타내면 그림 1과 같다. 그림 1는 4가지 유형의 가입자 네트워크 토폴로지를 나타내고 있으며, 초고속국가망/사용자망 접속점은 망관리 주체가 변경되는 경계점이다. 가입자망은 관리주체가 사설망 성격이 강하며, 또한 개인이 네트워크를 구축하여 운용하고 있다. 따라서 관리 책임은 개인 또는 특정 단체이다. 그러므로 이는 초고속국가

망 관리자와는 엄연히 다르므로 초고속국가망에서 제공하는 보안 기능의 경계점이라 할 수 있다.

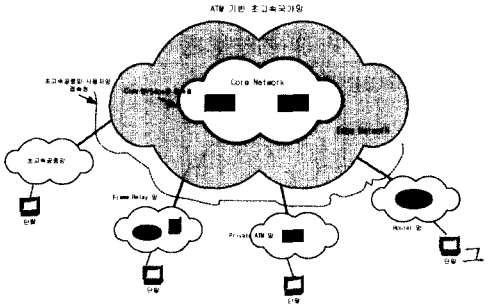

그림 1. 초고속국가망의 개념도

Ⅲ. 초고속망 가입자 정보보호 방안

초고속국가망 가입자 정보보호 방안은 가입자를 유형별로 분류하여, 각 유형별로 적합한 보안 모델을 검토하는 것이 바람직스럽다. 본 고에서는 가입자 네트워크를 제2장에서 검토한대로 사용 기능별로 3가지 유형으로 분류하고, 각 유형에 대해 3가지 네트워크 토폴로지를 적용한 가입자 네트워크로 구분하여 설명한다.

3.1 인터넷 백본 모델

초고속국가망에 접속되는 가입자 중 대부분이 전용선 형태의 Virtual Tunneling 기능을 이용하여 인터넷 백본으로 이용하고 있다. 이와 같은 목적으로 초고속국가망을 이용하는 가입자 네트워크에 대해 보안 기능 제공은 사용자 데이터에 대해 초고속국가망은 투명하게 제공해 주어야 한다. 따라서 이러한 목적으로 사용하는 가입자 그룹에 대한 보안 기능으로는 침입차단 시스템(Firewall)과 침입탐지 시스템(IDS:Intrusion Detection System)을 적용하는 것이 바람직하다. 데이터 링크 레벨 또는 물리 레벨에서 사용자 데이터의 암호화 기능 제공은 현실적으로 어렵다. 반드시 데이터 기밀성을 제공하기를 원한다면 상위 응용 계층에서 이루어져야 할 것이다 〈표 1〉.

표 1. 인터넷 백본으로 이용 시 적용 보안 기능

	침입차단 (firewall)시스템	응용 계층	사업자 (초고속국가망)
상호인증	X	O	O
기밀성	X	O	O
무결성	X	O	O
접근제어	O	X	X

O : 제공가능, X : 제공 불가능

초고속국가망에 접속된 가입자 네트워크 유형은 그림 1 및 그림 2와 같이 프레임릴레이망 가입자, 라우터망 가입자, Private ATM망 가입자 등으로 구분한다. 프레임릴레이 네트워크에 접속되어 있는 가입자 대부분은 LAN이며, 이는 라우터를 통해 프레임릴레이 네트워크를 경유하여 초고속국가망에 접속된다. 라우터망에 접속된 가입자(자사 LAN)는 라우터 및 라우터망을 경유하여 초고속국가망 접속 또는 라우터를 이용하여 직접 초고속국가망에 접속한다. Private ATM 네트워크 가입자는 직접 ATM 인터페이스를 통해 초고속국가망에 접속한다.

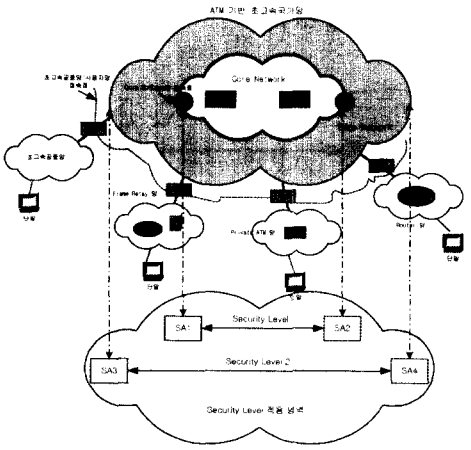

그림 2. 초고속국가망을 이용한 가입자 망 접속 개념도

초고속국가망에 접속되는 가입자 네트워크는 프레임릴레이망, 라우터망, Private ATM망으로 구성되는데, 현재 이러한 가입자 네트워크에서는 보안 기능을 제공하지 않고 있다. 따라서 보안기능을 제공하는 방안으로는 가입자 네트워크에 접속하기 위한 사용자(기관) 전용 인트라넷의 구성은 LAN 기반이며, 라우터를 이용하여 가입자 네트워크에 접속되는 구조이다. 보안 관점에서 보면, 보안의 책임은 최종단 사용자(End User)에게 있다. 따라서 가입자 레벨에서 보안 모델은 가입자 네트워크에 접속하기 전에 보안 기능이 이루어져야 한다. 따라서 ATM 가입자망에서 방화벽 적용 예를 그림3에 나타냈다.

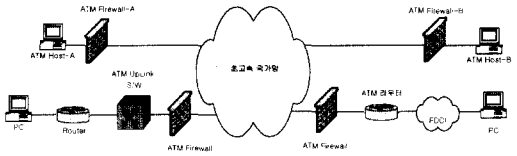

그림 3. 방화벽 적용 예

3.2 End Site간에 전용선 기능의 Virtual Tunneling 모델

본 방식은 인트라넷 기반의 VPN 구성의 일종이며, 초고속국가망을 통해 원격 지역 간을 접속할 때, 원격 지역 사이에 안전한 통신을 제공하는 것이 주 목적이다. 이 방법은 빈번히 발생하는 ATM 통신 환경에 적합한 ATM Site용으로 설계된 모델로 그림 4와 같이 SM(Security Module)을 각 ATM Site의 입구쪽 스위치에 두고서 원격 ATM Site 간을 보호하는 방법이다.

그림 4. End Site간 전용선 기능의 Virtual Tunneling 구현 모델

이 방식은 End-to-End간 점대점 연결방식에서 제공하는 보안모델로 VPN 방식의 일종이라 할 수 있다. 본 보안 모델에서 제공 가능한 기능을 정리하면 표 2와 같다.

표 2. End Site간 전용선 기능의 Virtual Tunneling 모델에서 보안 레벨

	Virtual Tunneling 시스템	응용 계층	사업자 (초고속국가망)
상호인증	O	O	O
기밀성	O	O	O
무결성	O	O	O
접근제어	O	X	O

O :제공가능, X : 제공 불가능

실제 초고속국가망 가입자 사이에서 Virtual Tunneling 기능 제공을 그림5와 관련해서 생각하면 다음과 같다.

① 초고속국가망 종단점에서 Virtual Tunneling 기능 제공 --- 그림5의 방법1
② 사용자가 가입자 네트워크 접속에서 Virtual Tunneling 기능 제공 --- 그림5의 방법2
③ 상기 ① 및 ② 기능을 동시에 제공하기 위해 Nesting 방식 적용

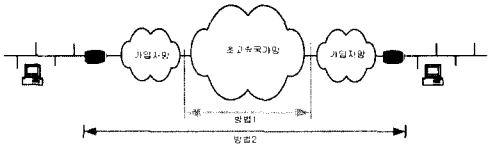

그림 5. End-Site간 Virtual Tunneling 기능 제공 방법

그림 5에서 방법1은 초고속국가망 사업자가 초고속국가망의 양 종단점 레벨에서 VPN 기능을 제공해 주는 모델이다. 이 경우는 초고속국가망과 가입자 망사이의 접속점 정합 장치에서 보안 기능을 구현함으로써 가능하다. 초고속국가망의 양 종단점 점에서 PVC 채널을 이용하여 제공한다. 또 다른 방법으로는 초고속국가망 가입자가 직접 End-to-End 간 Tunneling 기능을 제공하는 방법2를 생각 할 수 있다. 방법2는 최근에 사용화 되어 있는 방화벽에 구현된 VPN 기능을 이용하면 된다. 두 방식 모두 종단간 데이터 전송 시 상호 인증기능, 기밀성, 무결성, 접근제어 기능을 갖도록 구현 할 수 있다.

방식1과 같은 터널링 기술은 사업자 모델형이라 칭한다. 이는 사업자 망내에 설치되며, 가입자 망에는 VPN 기능이 없다. 방식2는 End-to-End 모델로 VPN 기능은 가입자 망에서 구현되며, VPN 기능은 가입자 네트워크에 접속되는 라우터 전단의 장비에서 제공된다. 따라서 사업자망은 전달망으로 연결 통로만 제공하는 방식이다.

3.2.1 방법1에 의한 Virtual Tunneling 구성 방법

초고속국가망에서 방법1과 같이 초고속국가망의 End-to-End간의 Virtual Tunneling 구성방법은 초고속국가망이 ATM 기반 네트워크이므로 PVC 채널 제공으로 가능하다. 이때 PVC 채널의 속도는 초고속국가망에서 가입자망과 접속점의 속도를 고려할 때, STM-1, DS3, E1 정도이다. 그리고 이 채널에 보안 기능 제공은 두 가지 방법으로 고려 할 수 있다.

① 초고속국가망 사업자가 보안 기능 제공 방법
② 가입자망 또는 가입자가 보안 기능 제공 방법

등이 있다. 초고속국가망 사업자가 보안 기능을 제공하는 방법은 PVC 종단 장치에서 SA(Security Agent) 기능을 갖도록 하고, 설정된 PVC 채널에 데이터 상호 인증 기능, 기밀성 제공, 무결성 기능 및 접근 제어 기능을 제공할 수 있다. 이때 필요한 보안 파라메터는 양단의 SA간에 협상을 통해 이루어진다. 이 방식은 초고속국가망에서 사용되는 Edge 교환기에 SA 기능을 구현하여야 가능하다. 현재 초고속국가망에서 사용하고 있는 ATM 교환기에는 이 기능이 구현되어 있지 않다.

초고속국가망 사업자가 형성된 PVC 채널에 보안 기능을 제공하지 않고, PVC 채널 양단에 상용 ATM 보안 장치를 이용하여 구성하는 방법이 있다. 현재 상용화되고 있는 ATM 보안 장치는 CeloTEK의 CellCase, GTE의 FASTLANE 등 몇 종류가 있다. 이를 이용한 구성 방법을 나타내면, 그림6과 같다. 그림6과 같이 구성할 경우, PVC 채널의 보안 특성은 양단에 사용한 ATM 보안장비의 특성에 의존하므로, 보안 정책과 관련하여 ATM 암호화 장치를 선택해야 한다는 점에 유의하면 된다.

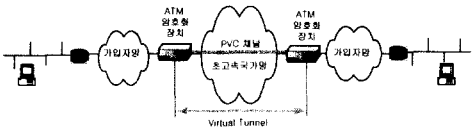

그림 6. ATM 암호장치를 이용하여 Virtual Tunneling 구성

3.2.2 방법2에 의한 Virtual Tunneling 구성 방법

프레임릴리이망을 이용하여 초고속국가망에 접속하기 위해서, 기관가입자의 경우는 내부 네트워크가 라우터를 통해 프레임릴레이망에 접속되고, 프레임릴레이망이 초고속국가망에 접속되는 형태이다. 이 경우에 각 기관사이의 End-to-End Site간 Virtual Tunnel 제공은 2단계로 이루어지고 있다. 1단계는 각 기관 접속점과 프레임릴레이망이 초고속국가망과의 접속점 간에 Virtual Tunnel이 제공되고, 2단계로는 초고속국가망의 양 종단점에서 PVC가 제공되어야 한다. 그림7과 같이 구성된다.

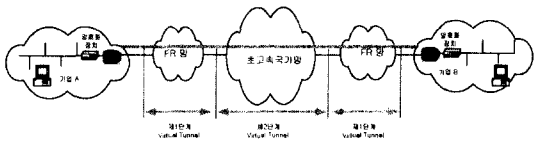

그림 7. 프레임릴레이 가입자망을 이용한 Virtual Tunnel 구성

그림7과 같이 End-to-End Site간 Virtual Tunnel를 구성한 다음에 VPN 기능을 제공하는 경우이다. 이와 같은 VPN 구성 방법은 계층2에서 구현하고 있다. 이때 형성된 채널에 대해 보안 기능 제공은 사용자에게 주어지므로, 외부 라우터 전단에서 보안 기능을 제공하면 된다. 요즈음 상용화 되고 있는 침입차단장치(Firewall)가 VPN 기능 겸용으로 제공되고 있으므로 인증기능, 암호기능, 무결성, 접근 제어기능을 제공할 수 있다. 즉 보안 정책에 맞게 가상 터널링을 구성한 다음에 보안 시스템을 구매하여 설치하면 된다. 또한, 그림7에 보인 암호화 장치 외에 라우터에 보안 기능이 첨가된 보안 게이트웨이를 이용하여 구성 할 수 있다. 이때 구성 방법은 제3 계층인 IPsec를 이용하여 구성 할 수 있다.

가입자 ATM 네트워크에 접속되어 있는 경우를 생각해 보자. 이때 기관 가입자 내부 네트워크이 어떻게 구성되어 있느냐에 따라 다르다. 여기서는 내부 네트워크가 ATM 백본으로 구성되어 있고, ATM 백본을 이용하여 10/100 Mbit/s 이더넷을 연결하고 있는 경우를 상상하자. 이때 초고속국가망과는 직접 ATM 인터페이스를 통해 STM1, T3, E1 급의 속도로 접속되고 있으며, 내부 네트워크간 사설 ATM 스위치의 정합장치에 의해 10/100 Mbit/s 이더넷을 접속 할 것이다. 이와 같은 구성을 그림8에 나타냈다. 그림8에서의 End-to-End Virtual Tunnel은 사설 ATM 네트워크의 양단의 ATM 스위치간에 PVC 채널을 구성하면 된다. 이 방식에서 구성된 가상회선(PVC)에 제공 가능한 보안 방식은 그림8과 같이 초고속국가망과 사설 ATM 스위치 사이에 ATM 보안 장치를 설치함으로 가능하다. 이 방식은 방식1에서 가입자가 보안 기능을 제공하는 방법과 같다.

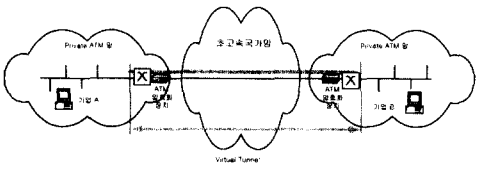

그림 8. Private ATM 가입자망을 이용한 Virtual Tunnel 구성

또 다른 유형으로 라우터망에 접속된 가입자의 경우에 End-to-End Site간 Virtual Tunnel를 구

성하는 경우는 그림 9와 같다. 초고속국가망을 통해 양 라우터 접속점 사이를 ATM PVC로 구성한다. 이때 사용하는 라우터는 ATM 인터페이스를 가지며, 속도는 STM-1, DS3, E1 등을 지원해야 한다. 또한, Frame Relay 인터페이스를 가질 수 도 있으며, 이때 속도는 E1급을 지원해야 한다. 그림9와 같이 구성된 네트워크에서 보안 기능 제공은 내부 네트워크에서 라우터에 접속되기 전에 암호장치를 설치하면 된다. 이러한 VPN 기능을 갖는 제품은 대부분 방화벽 기능과 함께 가지고 있으며, 사용자의 보안 정책에 따라 기능을 선택하도록 하고 있다.

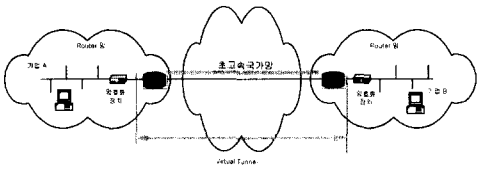

그림 9. 라우터 가입자망을 이용한 Virtual Tunnel 구성

3.3 VPN(Virtual Private Network) 기능

초고속국가망의 구조는 그림2와 같이 표현 할 수 있으므로, 초고속국가망 이용자 관점에서 VPN 구성은 전달계층에서 VPN를 구성하면, VPN 종단점 사이에서 고속의 통신 속도를 제공할 수 있다. 따라서 본 검토에서는 초고속국가망의 전달망 즉 링크 레벨에서 VPN를 구성할 때, 적용 보안 모델에 대해 검토 한다.

초고속국가망 가입자가 초고속국가망을 이용하여 VPN 구성할 때, 적용 가능한 보안 레벨은 표3과 같다. 이때 적용하는 보안 레벨은 초고속국가망 사업자가 제공할 수 도 있고, 초고속국가망 사용자가 별도의 보안 장치를 이용하여 제공할 수 있다. 현 시점에서는 초고속국가망 사업자는 PVC 기반의 가상 채널만 제공하고 있으므로, 사용자 입장에서 보안 장비를 이용하여 구성하는 것이 바람직하다. 이때 적용 가능한 보안 레벨은 VPN 가입자의 보안 정책과 보안 장비의 선택에 의존한다.

표 3. 초고속국가망을 이용한 VPN 적용모델에서 보안 레벨

	VPN 시스템	응용 계층	사업자 (초고속국가망)
상호인증	O	O	O
기밀성	O	O	O
무결성	O	O	O
접근제어	O	X	O

O : 제공가능, X : 제공 불가능

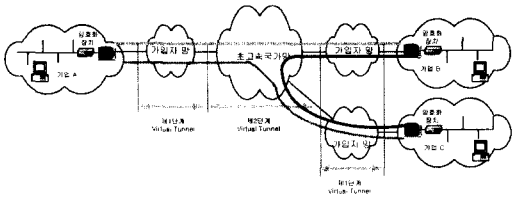

그림 10. 초고속국가망을 이용한 VPN 구성 개념도

초고속국가망을 이용하여 VPN를 구성하는 경우에 대해 구체적으로 살펴보자. 우선 그림10과 같이 인트라넷 기반의 VPN를 고려한다. 이때 초고속국가망에 접속되는 가입자 네트워크 유형은 이미 분석하였듯이 프레임릴레이망, 사설 ATM 망, 라우터 망으로 구분된다. 따라서 각 기업간(본사와 지사) 구성하는 VPN은 Full Mesh 형태로 가상 터널을 제공하여야 한다. 예를 들면 n개 그룹(본사 또는 지사)간에 VPN를 구성 할 경우, 각 그룹은 VPN 종단점에서 n-1개의 가상채널을 형성하여야 한다. 구성되는 가상채널은 가입자망 내 및 초고속국가망 내에서 형성되어야 한다. 이때 가입자망과 초고속국가망 사이의 접속점에서도 n-1개의 가상채널 접속점을 갖는다. 이상과 같이 가상채널이 구축되어 VPN이 전달망 레벨에서 구축된 경우에 대해 보안 모델을 구현하는 것이 바람직스럽다.

Ⅳ. 초고속국가망 정보보호 방안

초고속국가망은 ATM을 기반으로 한 네트워크로 Core 네트워크와 Edge 네트워크로 구성되어 있다. 또 초고속국가망 가입자는 별도의 가입자 네트워크에 소속되어 있으며, 가입자가 소속된 네트워크를 통해 초고속국가망에 접속되고 있는 형태이다.

초고속국가망의 보안은 초고속국가망 사용자 관점과 초고속국가망 네트워크 관점에서 본 보안으로 나누어 생각 할 수 있다. 네트워크 보안관점에서 고려하여야 할 파라메터는 일반적으로 송수신자의 상호인증, 기밀성 보장, 데이터 무결성 보장 및 접근제어로 나누고 있다. 이를 네트워크 보안 관점에서는 그림11과 같이 표현되는데, 네트워크의 제어평면과 관리평면 보안의 대부분은 망 제공자의 몫으로 주어진다. 그러나 사용자 평면의 제공은 망 제공자 및

가입자의 영역으로 양자가 데이터 보안을 책임질 필요가 있다.

그림 11. 네트워크 보안의 기능 적용 범위

	User Plane	Control Plane	Management Plane
Authentication			
Confidentiality			
Data Integtity			
Acess Control			

초고속국가망에서 사용자 데이터 보안은 사용자의 데이터 보안에 초고속국가망 제공자의 데이터 보안이 네스팅되는 개념으로 제공하는 것이 바람직하다. 여기서는 초고속국가망에서 제공하는 보안 개념에 대해서 설명한다. 초고속국가망은 ATM 기반 되어 있으므로, ATM 보안모델을 초고속국가망에 적용하여 검토하기로 한다.

초고속국가망에서 적용할 보안 개념은 최소한 2단계의 계층 구조를 갖는 네스팅 개념의 보안 레벨을 적용하는 방법을 생각 할 수 있다. 그림2에서 보면, 초고속국가망은 Core 네트워크와 Edge 네트워크로 구성되어 있다. 따라서 Edge 네트워크의 입·출력단과 Core 네트워크의 입·출력단에 SA(Security Agent)를 이용하여 네트워크 관점에서 보안을 강구하는 방법을 검토할 수 있다. 이 방법은 각 교환 모듈에 보안기능을 보완하는 방법으로 진행되어야 한다.

그림 2[제3장]는 보안의 네스팅 개념을 나타내고 있으며, SA1과 SA2사이에서 다시 보안 네스팅 개념을 적용할 수 있다. 또 SA1과 SA2를 포함하면서 SA3와 SA4 내부에서 보안 네스팅 개념을 적용할 수 있다. 제공하는 보안은 초고속국가망 사업자가 제공하여야 한다. 또 Edge 네트워크에서는 다양한 교환기가 이용되고, 초고속국가망에서 PVC 기능을 주로 사용하고 있기 때문에 가입자 네트워크와 초고속국가망 경계점에서 보안기능을 제공하는 방법을 생각 할 수 있다. 이 경우는 가입자 네트워크 쪽에서 초고속국가망과 접속하는 정합장치에 ATM 기반 보안 기능 혹은 다른 유형의 보안 기능을 제공하면 된다. 일반적으로 망 운용 관점에서 생각해 보면, 초고속국가망 사업자가 제공하여야 한다.

초고속국가망에서 보안 관리 방안은 그림12처럼 가입자가 초고속국가망에 접속하기 위해 원래 소속되어 있는 네트워크 유형과 가입자 성격으로 구분되는 이용기관별로 분류하였다. 이 분류 방법을 기본으로 초고속국가망에서 보안 관리방안을 도출하면 여러 가지 면에서 용이하다.

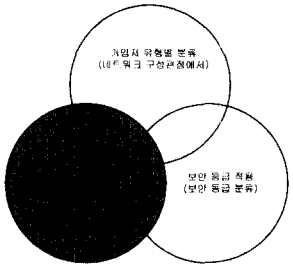

그림 12. 보안관리 방안 맵 구성도

V. 결 론

정보통신 네트워크에 있어서 안전신뢰성 대책이란 통신의 안정적인 제공, 통신 소통의 확보, 통신 비밀의 확보 등을 주목적으로 정보통신 네트워크를 둘러싼 다양한 위협이나 네트워크가 갖는 내부 취약성에 대해 네트워크의 내력을 강화하고, 그 기능의 안정적인 유지를 도모하는 것이다. 초고속국가망의 안전신뢰성 대책 측면에서 초고속국가망에 접속된 가입자를 유형별로 분석하고, 각 유형별 가입자 보안 방법을 검토하였다.

초고속국가망 가입자 유형을 네트워크 토폴로지에 따라 분류하면, 초고속국가망은 ATM 기반의 초고속 네트워크로 구성되어 있으며, 가입자 네트워크는 프레임릴레이망 가입자, ATM망 가입자, 라우터망 가입자로 구분하여 보안 기능 제공 방법을 분석하였다. 또 초고속국가망은 Core 네트워크와 Edge 네트워크로 나누고, 초고속국가망 내부에서 적용할 보안 개념 및 방법을 나타냈다.

가입자 유형별 최적 정보보호 방안 도출을 위해, 초고속국가망 가입자가 초고속국가망을 이용할 때 네트워크 서비스 유형을 3가지로 분류하고, 각 서비스 유형별로 3가지 네트워크 토포롤지에 대응하는 9가지 모델에 대해 정보보호 방안을 설명하였다. 이 때 제시한 서비스 유형별로 인터넷 백본 이용 모델, End-Site간 전용선 기능의 Virtual Tunneling 모델, VPN 이용 모델로 구분하였다. 각 서비스 유형별 모델에 대해 프레임릴레이망 가입자, ATM망 가입자, 라우터망 가입자 별로 정보보호 방안의 가이드 라인을 설명하였다.

향후, 초고속국가망의 이용 활성화를 위해 지금까지 설명한 보안 기능 제공 방안에 대해 보다 구체적이고, 현실적인 분석이 더 이루어져야 할 것이다.

참 고 문 헌

[1] ATM Forum, ATM Security Specification Version 1.0, af-sec-0100.000, February 1999.

[2] Laurent M., Rolin P., Stoffel L., Security Mechnism within Control Plane, Contribution ATM Forum/97-0040, February 1997.

[3] Carsten B., Uwd E., Securing Classical IP over ATM Networks, 7th USENIX Security Symposium, San Antonio, Texas, USA, January 1998.

[4] 한치문, 김기현, 김홍근, ATM Network Security 기술과 데이터 보호 방법, 정보통신지, 한국통신학회, 11월 1999.

[5] ATM Forum Technical Committee, ATM Security Framework 1.0, February 1998.

[6] K. McCloghrie, M.Rose, Management Information Base for Network Management of TCP/IP based internets, RFC 1156, May 1990.

[7] P. Ferguson, G. Huston, What is VPN?, The Internet Protocol Journal, April 1998.

[8] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.

[9] Watanabe, S. Seno, Y. Koui, T. Ideguchi, and M. Yabe, Realization Method of secure Communication Groups using Encryption, Transactions of Information Processing Society of Japan V.38 N.4, April 1997.

[10] A. Watanabe, T. Inada, T. Ideguchi and I. Sasase, Proposal of Group Search Protocol Making Secure Communication Groups for Intranet , ICC 2000, June 2000.

〈著者紹介〉

한 치 문 (Chimoon Han)
동경대학(The University of Tokyo) 대학원 전자정보공학부 공학박사
한국과학기술연구원(KIST) 연구원
한국전자통신연구원(ETRI) 선연, 책연 : 교환기술연구단 계통연구부장 역임
현재 한국외국어대학교 전자정보공학부 교수

이 형 옥 (Hyeong Ok Lee)
1996년 3월~1999년 8년 : 전남대학교 시간강사
1999년 2월 : 전남대학교 전산통계학과(이학박사)
1999년 10월~현재 : 한국전산원 국가정보화센터(선임연구원)