지리공간 유통망 보안 방안에 관한 연구

A Study on GIS Metwork Security

김 지홍* · 임 기욱**
Ji Hong Kim*, Gi Uk Lim**

요 약 지리공간 데이터 유통망 구조는 유통망 게이트웨이, 유통노드, 지리공간데이터 서버로 구성된다. 최근 정보통신기술과 네트워크 기술의 발전에 따라 점차적으로 지리공간 데이터 유통망에 대한 보안요구가 높아지고 있다.

본 논문은 지리공간 데이터 유통망 보안을 위하여 지리적으로 분산된 유통시스템에 대한 효율적인 접근통제방안을 제시하기 위한 방법으로 공개키 기반구조 기술을 이용하여 지리공간데이터에 대한 사용자별 접근통제방안과 지리공간 데이터의 전송보안을 위한 암호화 방안을 제시한다.

ABSTRACT The GIS Network consists of the Clearinghouse Network Gateway and Clearinghouse Node and Geo-spatial Data Server. Recently with the development of Information and Network technologies, GIS Network should be needed to be more secure than ever.

In this paper, we proposed the effective access control method for the distributed GIS network. PKI(Public Key Infrastructure) Technologies are used for access control and security for transmission on Geo-spatial data

키워드 : 지리공간유통망, 접근통제, 공개키기반구조

Ⅰ. 서 론

1995년 정부는 수치공간 데이터베이스의 개발과 지리정보의 표준화를 촉진시키기 위하여 국가지리정보체계(NGIS) 구축사업을 시작하였고, 현재 기본계획에 따른 지형도 전산화 사업과 기관별로 각종 주제도 구축이 완료되고 있으며, 이후 공간정보의 공유 및 활용에 대한 요구가 증가하고 있다. 또한 1999년도에 시행된 "공간정보 유통 및 활용에 관한 연구"에 따르면 197명의 설문 응답자중 95% 이상이 타 기관과의 공간정보공유를 원하고 있으며, 40 %이상이 이러한 정보를 수시로 활용하기를 원하고 있다[10].

또한 GIS 업무와 관련하여 공간정보데이터에 대한 보안요구조사에서도 고급보안요구(45.8%), 중급보안요구(28.4%), 저급보안요구(15.2%), 보안이 필요없음(26.4%)로 나타나고 있다[7].

이와같은 유통망에서의 보안요구에 따라, 본 연구는 지리적으로 분산된 각종 지리공간정보 데이터베이스에 대한 효율적인 접근통제 방법과 유통망에서의 전송보안부분을 논하고, 지리공간정보의 특성에 따라, 직무별 접근수준과 직급별 접근수준을 한정함으로서, 보다 안전한 지리공간 데이터베이스를 운영할 수 있도록 한다. 또한 최근에는 공개키기반기술의 암호이론, 인증이론과 기존의 다양한 접근통제기술을 병합하여 보다 효율적인 웹서버 및 데이터베이스에 대한 접근통제에 관한 연구가 활발히 진행되고 있다.

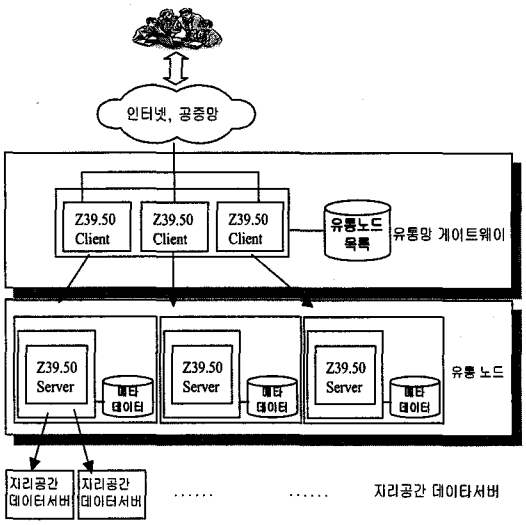
Ⅱ. 본 론

1. GIS 유통망 구조

국가 지리공간정보 유통망은 〈그림 1-1〉과 같다. GIS유통망을 구성하는 구성요소[8]는 인터넷망을 중

* 세명대학교 전자공학과 교수 jhkim@semyung.ac.kr
** 선문대학교 지식정보산업공학전공 교수 rim@etri.re.kr

심으로 GIS 유통노드를 관리하고 유지하는 유통망 게이트웨이와 사용자들에게 메타데이터의 검색과 공간데이터 서버를 연결해 주는 유통노드, 지리공간 데이터를 보관하고 있는 공간데이터 서버, 통신망 그리고 사용자로 나누어 볼 수 있다.



〈그림 1-1〉 지리공간 정보 유통을 위한 통신망

1.1 유통망 게이트웨이

유통망 게이트웨이는 유통망 시스템의 중추적인 역할을 담당하며, 유통노드목록을 보유하여 사용자가 원하는 지리공간 정보를 획득할 수 있도록 유통망 게이트웨이는 사용자와 유통노드 사이의 웹서버 기능을 하고, 메타데이터 서버로부터 메타데이터를 검색하기 위한 Z39.50 클라이언트 기능을 하며, 각 지역의 유통노드들의 목록을 보유하고, 메타데이터 검색을 위해 다양한 소프트웨어를 제공한다.

1.2 유통노드

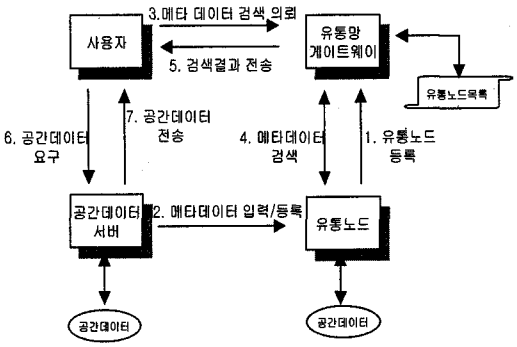
유통노드는 공간 정보에 대한 메타데이터 서버로서 Z39.50 서버기능을 한다. 또한 메타데이터 생성과 관리를 위한 표준화된 도구와 지침서를 공간데이터 서버에 제공하고, 공간데이터 서버로부터 공간정보에 대한 메타데이터를 입력받아 데이터베이스에 저장·등록하는 입력서버 기능을 한다.

1.3 공간데이터 서버

공간데이터 서버는 실제로 공간데이터를 저장하는 서버를 말한다. 사용자는 유통망게이트웨이의 웹서버 기능을 이용하여 공간정보를 보유하고 있는 기관의 공간데이터 정보를 의뢰할 수 있으며, 공간데이터 서버에서는 공간정보 브라우징 및 다운로드 서비스를 제공한다.

1.4 통신망

통신망은 유통망 게이트웨이와 유통노드간의 검색망과 지리공간 데이타 유통을 위한 전송망으로 구분할 수 있다. 검색망이란 유통망게이트웨이, 유통노드, 지리공간데이터서버간의 메타데이터 검색을 위해 제공되는 전용선 망을 의미하며, 전송망이란 실제로 사용자와 지리공간데이터서버간의 데이터를 전송하는 공개망을 의미한다.



〈그림 1-2〉 GIS 유통시스템

지리공간 정보유통망에 대한 접속과정은〈그림 1-2〉와 같다.

초기과정으로서 각 유통노드는 유통망게이트웨이에 접속하여 등록하고(1), 또한 각 공간데이터서버는 유통노드에 접속하여 자신의 공간데이터에 대한 메타데이타를 작성하여 등록한다(2).

사용자는 자신이 원하는 지리공간 데이터를 검색하기 위하여, 유통망게이트웨이에 접속하여 메타데이터 검색을 의뢰한다(3). 유통망게이트웨이는 Z39.50 프로토콜(4)을 동작시켜, 유통노드와 연결하여, 메타데이터 검색망을 통하여 여러 지역에 분포되어 있는 메타데이타를 검색하고(4), 이를 사용자에게 전달한다(5). 사용자는 유통망게이트웨이로부터 검색자료를 수신하여 유통망으로 필요한 지리공간데이터를 보유하고 있는 공간데이터 서버에 접속하여 데이터를 요구하고(6), 지리공간데이터서버로 부터 HTTP 혹은 FTP (File Transfer Protocol)을 이용하여 원하는 데이터를 다운로드 한다(7).

2. 접근통제 기술

접근통제의 목적은 컴퓨터 자원, 통신 자원 및 정보 자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다. 즉, 접근통제는 각 자원의 보호를 위해 기밀성(Security), 무결성(Integrity), 가용성(availability) 서비스를 제공하여, 사용자의 편의를 보장하면서 시스템 자원을 보호하는데 있다. 효율적인 접근통제를 위해서는 시스템자원의 가용성을 최소화하고, 사용자에게 많은 정보와 서비스를 제공하기 위해서는 자원의 가용성을 최대화하여야 한다. 또한 무결성과 기밀성을 보장하기 위해서 부가적인 장치가 도입되어야 할 것이다.

지리공간 유통노드에 대한 보안 방법은 1차적인 사용자 인증방법으로 유통망 게이트웨이에서 제공하는 ID와 Password를 사용하여 식별 및 인증과정을 거치고, 2차적인 사용자 인증방법으로는 지리공간데이터에 대한 접근통제방법으로 권한을 가진 사용자에게 공개키인증서를 검증함으로서, 권한에 해당되는 데이터를 제공하는 방법이 있다.

인증이 성공하면 각 시스템 자원에 대한 사용자의 요청을 보안정책이 적용된 접근통제 절차에 따라서 허용여부를 인가 받는다. 접근통제 시스템은 접근통제 서비스를 위한 접근통제 정책과 정책을 지원할 수 있는 접근통제 메커니즘을 필요로 한다.

접근통제 정책은 신분기반 정책(Identity- Based)과 규칙기반정책(Rule-Based Policy)으로 널리 알려져 있으며, 이 두 가지 정책을 혼합하여 직무기반(Role-Based Policy)정책으로 구분할 수 있다[11].

2.1 접근통제 정책

접근통제는 사용하는 주체에 따라 접근할 수 있는 범위를 제한하여 접근통제 정책을 수립하여야 한다. 이와 같이 접근통제를 위한 권한 설정방법은 최소권한정책(Minimum Privilege Policy)과 최대권한정책으로(Maximum Privilege Policy) 구분된다.

최소권한정책(Minimum Privilege Policy) 은 사용하는 주체에게 최소한의 권한만 부여하여, 접근 범위를 최소하여 데이터를 보안하는 방법이다. 최대권한정책(Maximum Privilege Policy)은 데이터 공유의 장점을 증대시키기 위하여 최대 가용성에 기반을 두었다. 즉, 사용자와 데이터 교환의 신뢰성 때문에 특별한 보호가 필요하지 않은 환경에 효과적으로 적용할 수 있다. 일반적으로 데이터베이스 보호를 위하여 사용자에게 접근통제기법으로 최소권한정책에 기반을 두고 있다.

2.1.1 신분기반 정책

신분기반 정책은 개인이나 그들이 속해 있는 그룹들의 신분에 근거하여 각기 다른 객체에 대한 접근을 제한하는 방법을 정의한다. 신분기반 정책은 개인기반정책(Individual-Based Policy)과 그룹기반 정책(Group-Based Policy)으로 분류하며, 개인기반 정책은 객체에 대한 사용자별 접근권한을 설정하는 방법이며, 그룹기반정책은 사용자에게 동일 목표에 대하여 그룹별로 일정한 허가를 부여하는 방식이다.

2.1.2 규칙기반 정책

규칙기반 정책의 각 객체는 보안등급(Classification Level)을 가지며, 사용자는 보안등급과 동일한 보안인가등급(Clearance Level)을 가지고, 주체와 객체가 갖는 보안등급의 정의를 통해 접근통제를 제공한다. 규칙기반 정책은 다중등급 정책(Multi-Level Policy)과 부서기반 정책(Compartment-Baed Policy)으로 구분된다. 다중등급 정책은 각 객체별로 지정된 허용등급(Classification)을 할당하여 접근통제를 제공하며, 부서 기반 정책은 업무단위인 부서별로 보안등급을 나누어 놓은 방식이다.

2.1.3 직무기반 정책(Role-Based Policy)

직무기반 정책은 신분기반 정책과 규칙기반정책을 혼합한 형태를 이루며, 신분기반 정책의 그룹기반 정책과 유사하다. 즉 정보에 대한 접근 권한은 개별적인 신분에 의하여 접근하는 것이 아니라, 부서 내에 개인의 직무의 성격에 따라서 결정된다.

3. GIS 공간정보 유통구조에서의 접근통제방안

3.1 공개키 기반구조(PKI : Public Key Infrastructure)

암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털인증서를 통해 사용자를 인증하는 시스템이다. 이는 전자거래나 정보유통의 안전성과 신뢰성을 확보하기 위한 방법으로, 제 3의 공인신뢰기관을 두어 상대방의 신원을 확인하고 정보내용의 변경확인과 비밀유지기능을 갖는 지식정보화 사회의 핵심기반이다.

공개키기반구조[7,9]는 공개키에 대한 인증서를 발급하는 인증기관(CA : Certification Authority), 사용자들의 인증서 신청시 인증기관 대신 그들의 신분과 소속을 확인하는 등록기관(RA : Registration Authority), 인증서와 사용자 관련정보, 상호인증서 및 인증서 취소목록(CRL : Certificate Revocation) 등을 저장 검색하는 장소인 디렉토리, 또한 다양한 응용

에서 공개키를 이용하여 전자서명을 생성하고 검증하며 데이터에 대한 암호, 복호를 수행하는 모듈 등이 포함된다.

3.2 GIS 공간정보의 접근통제 방안

GIS 유통기구(Clearinghouse)를 주축으로 한 유통노드간의 검색망 뿐 아니라 인터넷을 이용한 사용자들에게 신뢰성과 안전성을 부여하기 위해서는 GIS 유통기구들에 대한 인증기능이 부여되어야 한다. GIS 정보의 안전한 유통을 위해 공인인증기관을 통하여 GIS 관련기관에 인증서를 발급하여, GIS 사용자들을 위하여 GIS 인증서를 관리하고, 인증 실무준칙을 저장하기 위한 인증기관인 PCA (Policy Certification Authority)가 구성되어야 한다. GIS PCA는 안전한 지리정보 유통을 위한 보안알고리즘과 유통노드에 대한 접근 통제 역할을 수행할 수 있도록 GIS 인증서 발급 및 관리를 위해 인증실무준칙을 제정하는 역할을 하며, 지리정보유통망의 관문이 되는 Clearinghouse 역할도 함께 수행 할 수 있다.

3.2.1 공개키기반구조에서의 인증 방법

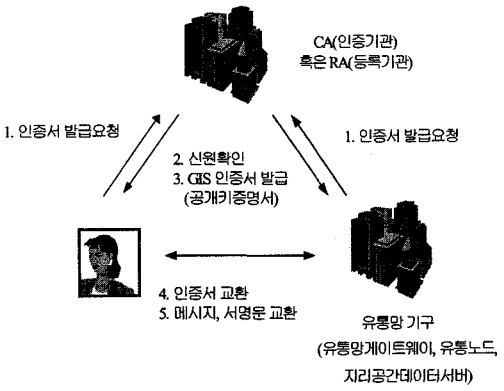
공개키 인증서는 공개키기반구조내의 상위 인증기관이 하위 인증기관에게 발급하는 CA 인증서와 인증기관 혹은 등록기관을 통하여 사용자들에게 분배하는 사용자 인증서, 인증기관 간의 상호 인증서 등으로 분류되며, 용도에 따라 전자우편용 인증서, 금융거래용 인증서, 전자상거래용 인증서, 일반 사용자용 인증서, GIS용 인증서 등으로 분류되며, 인증서 형식은 IETF(Internet Engineering Task Force)에서 제정한 X.509 v3 형식[9]을 따른다. 지리공간정보 유통망에서 사용되는 GIS 공개키인증서는 기존의 X.509 v3 공개키 인증서에 대한 지침을 사용하며, 다만 인증서 확장자 영역에서 주체와 발급자에 대한 속성 정보에 해당되는 주체 디렉토리 속성(Subject Directory Attribute) 필드를 이용하여 사용자의 소속, 직무, 직급에 관한 정보를 기재하는 것으로 GIS 유통망에서의 데이터베이스 접근통제를 위하여 사용된다. 이는 다음 절에서 소개될 지리공간데이터에 대한 접근통제를 위하여 적용될 사용자별 권한정보 자료로 사용된다.

가. 인증서 발급과정

사용자는 인증기관 혹은 등록기관으로부터 자신을 입증할 수 있는 신분증을 제출하여 신원확인과정을 거쳐야 인증서를 발급 받을 수 있으며, 인증기관이나 등록기관은 상위 인증기관으로부터 지정된 절차에 의해 확인과정을 거친 후, 공개키 인증서를 발급 받을 수 있다. 이러한 과정은 〈그림 3-1〉과 같다.

나. 인증서 검증과정

공개키 기반구조에서의 인증서 검증은 수신된 인증서를 발행한 인증기관(CA)에 대한 공개키를 획득하여야 상대방의 공개키 인증서에 대한 검증절차를 시행할 수 있다. 왜냐하면 공개키 인증서는 발행시에 인증기관의 개인키를 이용하여 서명하기 때문에 인증서를 발행한 인증기관의 공개키를 가지고 인증서를 검증할 수 있다. 상대방 인증서를 발행한 해당 인증기관의 공개키를 얻기 위해서는 명명구조(naming structure) 방법를 이용하여 신뢰지점(trusted point)을 찾고, 신뢰지점으로부터 계층구조상의 인증서 체인을 획득하는 방법이 사용된다[9]. 이와같은 방법으로 상대방 CA의 공개키를 획득하여 수신된 인증서를 검증한 후에는 반드시 인증서 취소목록을 검색하고 해당 인증서의 유효성을 검증하여야 한다. 이러한 절차에서 문제점이 발생되지 않으면, 상대방에 대한 인증이 완료된 것으로 간주하며, 인증서의 확장영역에 기록된 직무영역 및 직무등급과 직급등급에 대한 데이터를 추출하여 데이터베이스에 대한 접근통제를 위한 기초데이터로 사용한다.

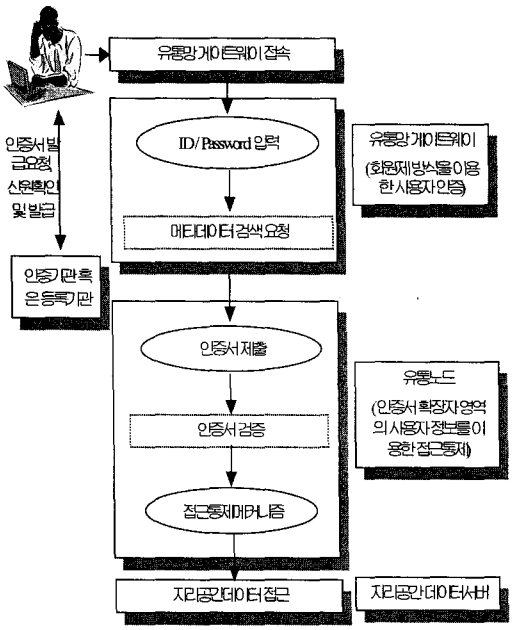


〈그림 3-1〉 인증서 발급과정

다. 지리공간유통망 접근통제와 사용자 인증

유통망에 대한 접근통제 및 사용자 인증은 〈그림 3-2〉와 같이 구성된다. 먼저 인터넷상에서 유통망 게이트웨이, 유통노드 및 지리공간 데이터서버는 공개키 기반구조 상의 GIS PCA 인증기관으로부터 인증서를 발급받고, 인증서를 사용하여 신뢰체인을 형성할 수

있다. 유통노드가 유통망 게이트웨이에의 등록절차, 지리공간 데이터서버의 유통노드로의 메타데이터 입력 절차 등의 과정에서 유통기관 간의 인증절차를 거친다. 마찬가지로 사용자도 인증기관으로부터 GIS 인증서를 발급받고, 이를 이용하여 유통망에 접속하여 인증서를 교환함으로서, 상호간의 신뢰를 구축할 수 있다. 이와같이 지리공간 데이터 사용자가 GIS 유통망을 통하여 지리공간 유통망 접근통제와 사용자 인증은 다음과 같이 설명될 수 있다



〈그림 3-2〉 GIS 지리공간 데이터서버 접속과정

(1) 유통망게이트웨이에 접속하여 유통노드 또는 지리공간 유통망에 접속하기 위해서는 자신의 ID와 패스워드를 입력하는 1차 사용자 인증 과정을 거친다.

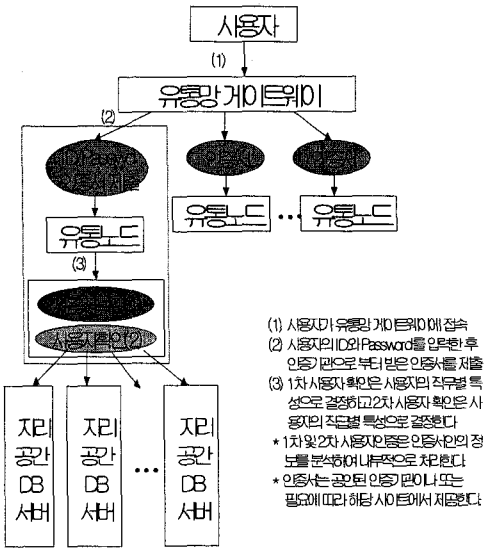
(2) 지리공간 데이터 사용자는 메타데이터 검색을 위하여 유통노드에 접속한다.

(3) 유통노드에서는 자신의 인증서를 사용자에게 제출하여, 신뢰성있는 기관임을 확인시킨다. 또한 유통노드에서는 사용자의 신원확인을 위하여 사용자인증서를 요청한다. 이와같이 상호간의 인증서 교환과 검증을 통하여 상호간에 신뢰된 객체임을 확인하고, 유통노드에서는 사용자에 대한 접근권한을 설정하기 위하여, 사용자인증서의 확장영역에 기술된 직무등급과 직급등급에 대한 데이터를 분석한다.

(4) 필요로 하는 지리공간 데이터를 소유하고 있는 지리공간데이터 서버에 접속할 경우에는 (3)번에서 분석된 사용자 정보를 이용하여 접근가능여부를 결정한다.

(5) 접근이 인가된 사용자에 한하여, 지리공간데이터 서버에 접속을 허용하고, 과금여부를 결정한다. 접근이 끝난 경우에는 로그아웃 방법을 이용하여, 강제로 세션을 해지한다.

〈표 3-1〉은 유통망시스템의 데이터를 보호하기 위해 접근통제 알고리즘의 위치에 따른 장·단점을 분석하였다.



〈그림 3-3〉지리공간정보 유통망에서의 접근통제 방안

〈표 3-1〉 GIS 유통망에서의 접근통제 기능의 위치

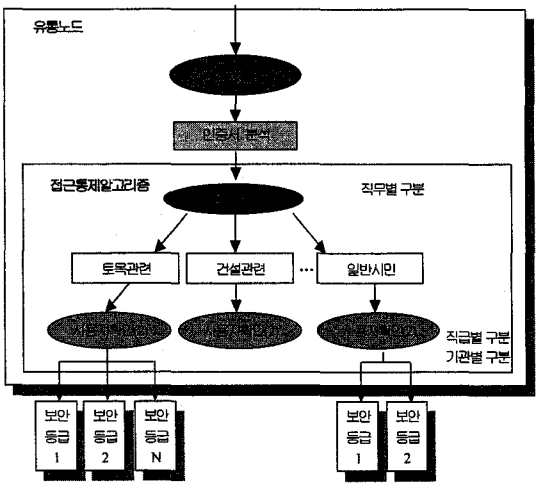
	유통망 게이트웨이	유통노드	지리공간 DB서버
장점	■유통망 전반에 대한 접근통제가 가능하다.	■트래픽 현상이 분산됨에 따라 원활한 서비스를 제공할 수 있다.	■지리공간데이터에 대한 접근통제가 수월하다
단점	■ 유통노드 및 지리공간 DB서버에 대한 별도의 보안 대책이 필요하다. ■ 해킹이나 보안공격으로 인해 전체 서비스가 단절된다.	■유통노드에서의 부하증대 ■ 유통망게이트웨이에 대한 ID/Password 인증기능 추가	■ 유통노드에 대한 별도의 보안 필요 ■ 모든 DB에서 사용자에 대한 접근통제를 수행함으로써 설치비용이 증가한다.

라. 접근통제 메커니즘

유통노드에서 지리공간 데이터베이스에 대한 접근통제는 1차 접근통제와 2차 접근통제로 구분된다. 또한

객체 데이터의 보안등급(Classification)은 건설교통부에서 제정한 〈건설교통부훈령 제313호 국가지리정보 보안관리규정〉[5]에 의거하여 "공개", "공개제한", "비공개"의 3등급으로 분류하였고, 사용자에 대한 접근통제는 보안인가등급(Clearace)을 부여하여 관리한다.

접근통제 방법으로써 1차 접근통제는 직무별 사용자 접근통제에 해당되고, 2차 접근통제는 직급별 사용자 접근통제에 해당된다. 본 논문에서는 1차 직무별 접근통제를 위하여 사용자의 보안인가등급(clearance)을 다음과 같이 분류하였다. 데이터 보유기관, 유관기관, 기타 사용자로 분류하였다.



〈그림 3-4〉 유통노드에서의 접근통제 방향

1) 데이터 보유기관
① 데이터 관리부서에서의 접속
(직무별 직무권한 = 4)
② 기타 부서에서의 접속 (직무별 직무권한 = 3)
2) 유관기관
① 동일 부서에서의 접속 (직무별 직무권한 = 3)
② 기타 부서에서의 접속 (직무별 직무권한 = 2)
3) 기타 일반사용자 (직무별 직무권한 = 1)
4) 특수사용자 (직무별 직무권한 = 1,2,3)

데이터 보유기관이란 지리공간 데이터서버를 보유하고, 해당 데이터에 대한 관리를 실행하고 있는 기관을 의미하며, 유관기관이란 해당 데이터를 직접 관리하지는 않지만 그 데이터와 관련이 있는 부서(기관)를 의미한다. 일반사용자는 공개된 지리공간데이터를 열람하고자하는 사용자를 의미하며, 공개되지 않는 지리공간데이터를 열람하고자 하는 사용자는 특수사용자로 취급되며, 별도의 신청절차를 통하여 접근권한이 부여되는 사용자를 의미한다.

데이터베이스에 대한 접근방법은 일반적으로 "Retrieve", "Update","Insert","Delete" 방법이 있다. 데이터보유기관의 경우에는 "비공개", "공개제한", "공개" 데이터에 대하여 직급별로 "Retrieve", "Update", "Insert", "Delete" 권한을 부여하고, 유관기관의 사용자에게는 기본적으로 "비공개", "공개제한", "공개" 데이터에 대하여 직무별 특성에 따라 선택적으로 "Retrieve" 권한을 부여하는 방식을 적용하였다.

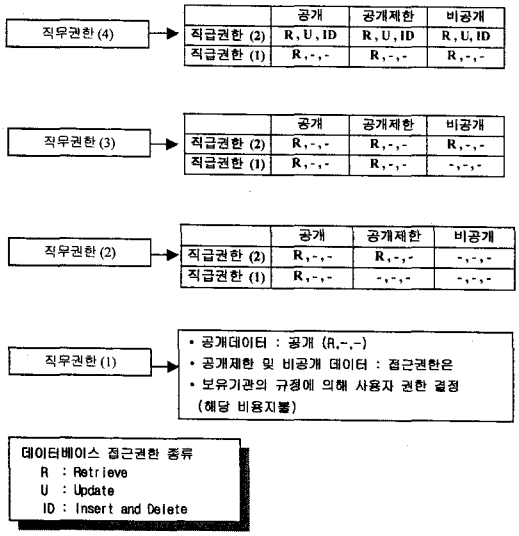
기타 일반사용자의 경우에는 기본적으로 "공개" 데이터에 대해서만 "Retrieve" 기능을 가지게 한다. 그러나 "공개제한" 혹은 "비공개"에 해당되는 지리공간데이터에 대하여 "Retrieve" 기능을 필요로 하는 특수사용자는 지리공간 데이터를 소유한 해당 기관에 요청하고, 해당 기관에서는 이러한 요구를 심사하고 해당 데이터에 대한 접근권한을 부여할 수 있다. 이와 같은 기준은 최소권한 정책에 의거하여 임의로 작성한 것이므로, 부서별 특성에 따라 공간정보 계층별 데이터에 대한 보안수준에 의거하여 지정할 수 있다.

〈표 3-2〉 직무별 접근통제방안

	공개	공개제한	비공개	비 고
직무권한 (4)	R,-,-	R,-,-	R,-,-	직급에 따라 U, ID 기능 부가
직무권한 (3)	R,-,-	R,-,-	R,-,-	데이터수정불가
직무권한 (2)	R,-,-	R,-,-	-,-,-	데이터수정불가
직무권한 (1)	R,-,-	-,-,-	-,-,-	데이터수정불가

2차 접근통제는 직급별 접근통제방식이다. 직급별 보안인가 등급을 부여하기 위하여 안 책임자 및 담당부서장(직급별 직급권한 : 부서 담당자 및 관리자(2), 기타 부서직원(1))로 분류하여 객체 데이터에 대한 접근통제 방법을 〈그림 3-5〉와 같이 제안하였다.

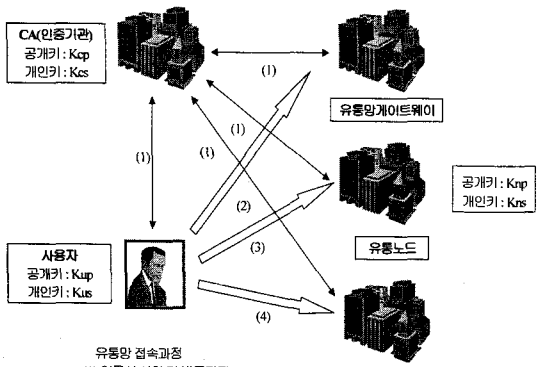
GIS DB 서버에 대한 직무·직급별 접근통제 알고리즘을 사용하는 이유는 DB서버에 대한 여러 기관의 공유문제를 해결하기 위함이다. DB 서버를 관리하는 기관이 아닌 유관기관 또는 타기관에게 자료 검색 서비스를 제공하기 위해 직무별 알고리즘을 사용하고, DB 서버 데이터에 대한 추가, 변경, 삭제 등을 할 수 있는 관리자와 단순히 검색 서비스만을 이용하는 일반사용자를 구분하기 위해 직급별 알고리즘을 사용하였다.



〈그림 3-5〉 직무/직급별 접근통제방안

4. 공간정보유통망에서의 전송보안

GIS 유통시스템은 사용자, 공간정보 검색을 위한 창구역할을 하는 유통망 게이트웨이, 메타데이터를 보관하는 유통노드, 실제 계층별 데이터를 보관하는 공간데이터 서버로 구성된다. 접근통제 알고리즘에 관해서는 전 장에서 설명된 바와 같이 직무특성에 따라, 직무권한과 직급권한을 이용하여 접근통제를 실시할 수 있으며, 본 장에서는 유통노드에서의 메타데이터 수신시의 암호화 방안과 유통데이터서버로부터의 공간데이터 수신시의 암호화 방안을 검토한다.



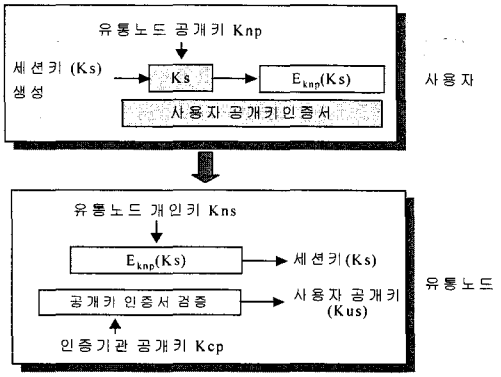
〈그림 4-1〉 GIS 지리공간 데이터서버 접속과정

4.1 유통노드에서의 전송보안

사용자가 유통망게이트웨이에 접속하여 유통망과 관련된 기본적인 정책 및 도구 등에 대한 자료를 얻을 수 있으며, 실제로 지리공간데이터를 열람 혹은 다운로드 받기를 원하는 경우에는 인증기관으로부터 GIS용 공개키 인증서를 발급받아야 한다. GIS 공개키 인증서는 기존의 공개키 기반구조에서 유통망 접근통제를 위하여 인증서 확장자 영역의 주체 디렉토리 속성(Subject Directory Attribute) 정보영역에 GIS 사용자에 대한 권한정보(사용자의 소속, 직무, 직급)를 저장한 것으로 특성화된다. 이러한 정보는 기본적으로 지리공간 데이터베이스에 대한 접근권한을 규정하는데 사용되며, 접근통제알고리즘에 직접 적용된다.

4.1.1 세션키 공유방법

사용자와 유통노드간의 전송되는 메세지 및 메타데이터 전송시에 세션키를 사용한다. 세션키란 일종의 무작위 난수(random number)로서, 키생성기에 대한 초기값(seed vector)로 사용될 수 있으며, 실제로 사용자와 유통노드간의 해당 세션동안의 데이터 전송을 위하여 사용되는 암호화키를 의미한다. 세션키는 사용자 혹은 유통노드 측에서 임의로 생성될 수 있으나, 전송프로토콜의 간소화를 위하여 사용자가 임의의 세션키를 생성하여, 유통노드의 공개키를 이용하여 암호화하여 전송하며, 유통노드에서는 자신의 개인키를 이용하여 이를 해독함으로서 해당 세션동안의 데이터 암호화를 위한 세션키 공유방법이 사용된다. 이러한 과정은 〈그림 4-2〉와 같다.

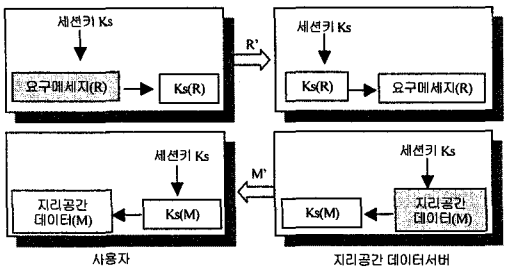


〈그림4-2〉 사용자와 유통노드간의 세션키 공유방법

4.1.2 사용자와 유통노드간의 데이터 암호화방법

4.1.1에서 설명된 바와 같이 송수신데이터를 암호화하기 위한 세션키를 공유한 후의 모든 데이터는 세

션키를 이용하여 데이터를 암호화하여 전송한다. 메타데이터는 사용자가 원하는 지리공간정보에 대한 이력정보를 검색할 수 있으며, 또한 지리공간 데이터에 대한 소개 및 광고효과도 누릴 수 있으므로, 인증기관으로부터 GIS 공개키 인증서를 발급 받은 사용자에 대해서는 기본적으로 공개함을 원칙으로 한다. (보안알고리즘으로는 Z39.50 메타데이터 교환프로토콜에서 제공되는 DES 알고리즘을 사용한다[9].)

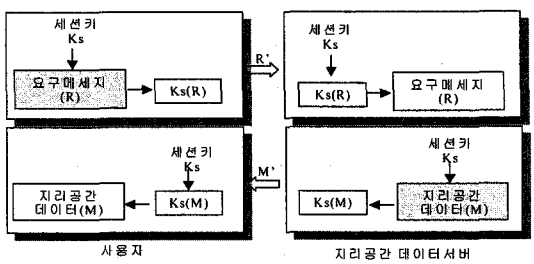


〈그림 4-3〉 사용자와 유통노드간의 데이터 암호화 방법

4.2 지리공간 데이터서버에서의 전송보안

유통노드에서 해당 사용자의 GIS 공개키인증서를 통하여 기본적인 접근권한이 지정된다. 사용자는 지리공간 데이터서버와 접속하여 데이터를 전송하기 위해서는 세션키를 공유하고, 해당 세션키를 이용하여 지리공간 데이터를 암호화하여 전송한다.

사용자의 지리공간데이타 요구메세지는 세션키를 이용하여 암호화되어 지리공간 데이터서버에 전달되며, 유통노드에서는 세션키를 이용하여 요구메세지를 해독한다. 마찬가지로 지리공간 데이터서버에서는 요구된 지리공간데이터를 세션키를 이용하여 암호화하여 사용자에게 전달하며, 사용자는 세션키를 이용하여 복호한다. 이와같이 지리공간데이터 암호화방법은 〈그림 4-4〉과 같다.



〈그림 4-4〉 사용자와 지리공간데이터서버의 데이터 암호화 방법

Ⅲ. 결론

본 논문에서는 인터넷의 활용이 증가하면서, 널리 분포되어 있는 지리정보의 효율적인 관리를 위해 접근통제 기술을 통한 GIS 유통시스템의 관리에 대하여 알아보았다. GIS 유통 시스템은 사용자로 하여금 메타데이타를 검색을 위해 유통노드와 연결해주는 유통망 게이트웨이, 공간데이타 서버로부터 메타데이타를 입력받아 유지·관리하면서 메타데이타 검색 서비스를 하는 유통노드, 공유가능한 정보를 보관하여 사용자들에게 HTTP와 FTP 서비스를 제공하는 공간데이터 서버로 구분 할 수 있다.

GIS 공간정보 유통구조에서의 접근통제방안을 강구하기 위하여, 공개키기반구조를 이용한 접근통제방안을 제안하고, 유통망에서의 접근통제와 유통노드에서의 접근통제를 제안하면서, 인증서에 기록된 사용자 직무 및 직급별 정보를 이용하여 사용자 접근권한에 따라 계층별 지리공간데이터에 대한 접근을 가능하게 하는 방식을 제안하였다. 또한 지리공간데이터의 암호화를 위한 세션키 공유과정과 세션키를 이용한 지리공간 데이터의 암호화 방법 및 암호화 기법을 소개하였다. 본 논문에서는 안전한 지리공간정보 유통망 구축을 위해서 각 레이어별 접근통제 방법을 제시하였다. 이러한 접근방법은 지리공간정보 유통망을 통하여 보다 안전하고 신뢰성 있는 지리공간 데이터를 보장함으로서, 향후 지리공간 유통을 이용한 관련 산업분야의 발전에 기여할 것으로 기대된다.

참고문헌

[1] FGDC, "The FGDC Standard forDigital Geospatial Metadata",1999.11.

[2] IETF, Security Area, "X.509 (pkix) Document", http://www.ietf.org, 1999.7.

[3] ISO-TC211, "Geographic Information", http://www.statkart.no/isotc211, 1999.

[4] US Library of Congress, "The Z39.50 Standard, Related Agreements, Amendments, Etc", 1999.

[5] Z39.50 Maintenance Agency, "Information Retrieval (Z39.50)", 1995.

[6] 건설교통부, 건설교통부훈령 제313호, "국가지리정보 보안관리규정", 2001.1.30

[7] 김지홍, "지리공간 정보유통을 대비한 정보보호 정책연구", 기업정보화지원센터,1999.

[8] 성기석, "국가 지리공간정보의 유통체계 구축 및 전략연구", 기업정보화지원센터, 정보통신부, 1999.
[9] 이만영, 김지홍, 류재철, 송유진, 염흥렬, 이임영, 전자상거래 보안기술, 생능출판사, 1999.
[10] 정승렬, "공간정보 데이터웨어 하우스 구현을 위한 정책연구", 기업정보화지원센터, 정보통신부, 1999.
[11] 한국정보보호진흥원, "접근통제기술 개요", 1999.

김지홍(金志弘)

한양대학교 전자공학과 졸업
한양대학교 전자통신공학 석사
한양대학교 전자통신공학 박사
1982-1991 엘지전선연구소 근무
1995.2 정보통신기술사
1991-2002.8 세명대학교 전자공학과 교수
2002-현재 세명대학교 정보보호학과 교수
1999-2001 한국정보보호학회 논문지편집이사
2001-현재 한국정보보호학회 총무이사
관심분야: 공개키기반구조, 접근제어, 네트워크보안,

임기욱(林基郁)

인하대학교 공과대학 전자공학과 졸업
한양대학교 전자계산학 석사
인하대학교 전자계산학 박사
1977-1983 한국전자기술연구소 선임연구원
1983-1988 한국전자통신연구소 시스템소프트웨어 연구실장
1988-1989 미 캘리포니아 주립대학(Irvine) 방문연구원
1989-1997 한국전자통신연구원 시스템연구부장
주전산기(타이컴) III, IV 개발 사업책임자
1997-1999 정보통신부 정보통신연구진흥원 정보기술전문위원
2000-현재 선문대학교 지식정보산업공학전공 교수
2001-현재 ETRI 컴퓨터소프트웨어연구소장

관심분야: 실시간 데이터베이스시스템, 운영체제, 시스템구조