인트라네트 동향과 데이터베이스(2)

이용호/대한무역투자진흥공사 정보사업부장

인터네트(Internet)의 기술은 조직내부의 문제를 현실로 받아들여야 하는 상황에서 아주 유익한 조직력을 스스로 발휘하는 수단이 된다.

지금까지 셀 수도 없이 많은 정보시스템(Information System이라 하여 보통 IS라고 함)이 '인트라네트(INTRANET)'라 불리는 방화벽(Firewall)의 뒤단에 숨겨놓은 다음 세대 정보시스템으로 인터네트와 웹 기술을 이용하고 있다.

기존 시스템을 웹(WEB)으로 바꿔가는데 정보 시스템에 있어서의 이러한 새로운 움직임은 데이터베이스, 그룹웨어, 워크플로(WorkFlow)와 같은 응용소프트웨어에 새로운 활기를 불어넣고 있다.

최근 논란의 초점이 되고 있는 PC 기반의 인터네트와 네트워크컴퓨터 기반의(Network-Computer based) 인터네트 중 어느 것이 이 시대를 주도해 나갈 것인가에 따라 인트라네트 구축용 소프트웨어 또한 달라질 것이고, 국제적인 소유권 문제를 더욱 모호하게 해놓을 가능성이 있다.

사실 인터네트와 인트라네트는 서로 똑같은 표준화된 기술을 사용하고 있지만, 자세히보면 이들은 서로 근본적인 차이가 있다. 인트라네트는 인터네트에 어느 정도 길들여진후 조직내에 새로운 부가가치로 주어진다는 점이 다르다.

아울러, 인터네트를 이용 데스크톱에서 자유자재로 쓸 수 있는 모든 응용소프트웨어로부터의 자유 즉, 정보자원의 조직적 접근이 가능해야만 추진이 가능하다는 점이다.

다가올 인터네트 사회(INTERNET SOCIETY)에 대해 많은 전문가들은 인터네트상에 연결되어 있는 호스트 컴퓨터 수(Hosts)로 판단하고 있는데, 1991년대 40만대 호스트 수가 1995년에는 4백8십만대로 늘어났고 다가오는 2000년대는 2억대의 호스트 컴퓨터가 인터네트의 서버용 컴퓨터로 서로 연결될 전망이라고 한다.

이번호는 지난호에 이어 두 번째로 인트라네트의 구축방법과 보안환경에 대해 기술해 보겠다.

인트라네트 구축방법론

글로벌네트워크 시대에 맞는 인공지능학의 한 분야인 ES(Expert System)에서 흔히 사용하는 전형적인 질의도 웹상의 질의 형태로 바꿔야 할 것 같다. 예를 들어 "동아시아, 북유럽, 미주에서 판매된 컬러 TV는 총 몇 대인가?" 미주에서 실제 판매된 컬러 TV는 목표로 한 판매량의 몇 % 정도인가? 등의 질의가 웹(Web) 상에서도 아무런 제약없이 사용될 것이다.

그러나 사용자들은 매우 빈번하게 조건식의 조합를 요구한다. 예를 들어 아시아 지역의 컬러 TV 판매율이 유럽시장의 작년 판매율과 같은 속도로 성장한다면 올해 아시아 지역 컬러 TV 판매액은 어느 정도일까, 아시아 지역의 영업사원을 3명 보강한다면 컬러 TV 판매액은 어느 정도 일까, 이에 대한 답을 할 수 있어야 할 것이다.

기존 클라이언트/서버 시스템의 큰 문제는 자료간의 비호환성으로 요약할 수 있다. 각 제품마다 데이터에 대한 독자적인 파일 포맷을 갖고 있어 이로인해 확장에 많은 문제점을 가져왔다.

독자적으로 그룹웨어를 구축해 오던 상급기관과 하급기관이 결국에는 서로간의 정보 교환을 위한 확장의 방법을 찾아내지 못하는 경우가 많았다. 이러한 문제를 미리 예방하기 위해서는 결국 전사적인 차원의 인트라네트 수립을 기획을 해야 한다. 이는 비록 구축을 위한 도입 기간이 길게 걸릴지라도 계속적인 새로운 기술의 적용을 위해서라도 필요한 것이다.

다음은 몇가지 인트라네트의 구축의 기술적인 특성들이 있다. 이러한 특성을 이해하는 것이 인트라네트 시스템 구축 계획을 세우는데 필요한

중요한 아이디어를 제공해 줄 수 있을 것이다.

그 방법론을 간략하게 요약하면 글로벌 액세스, 쉬운 사용법, 유연성, 오픈시스템, 크로스 플랫폼, 다양한 멀티미디어/객체지향 기술지원 등으로 정리해 볼 수 있다. 구축시에는 다음과 같은 방법과 수순을 발견할 수 있다.

첫째, 인트라네트는 표준화된 플랫폼으로 확장성을 가질수 있어 단계적으로 접근하는 방법이다.

둘째, 웹브라우저의 통일로 시스템 관리자의 부담을 경감시키며 통일화된 전략으로 추진하는 방법이다.

셋째, 사용자도 직접 정보의 생산자가 될 수 있으며 광범한 분산환경이 가능해질 수 있도록 구축하는 방법이다. 즉, 사용자가 정보의 생산, 편집, 관리 등의 체계가 먼저 제도적으로 선행되어야 한다.

넷째, '사기전에 시험해보라'는 인터네트의 관행으로 경제적인 테스트베드 구축을 우선 추진한 후에 전체로 확산 시키는 방법 등이다. 이것은 위험 부담을 줄이고 사용자에 가장 적절한 시스템 구축으로 유도할 수 있다.

인트라네트의 구현기술

새로운 데이터베이스 모델의 탄생

인트라네트에 있어서 중요한 과제는 지난 수년간 구축된 기업데이터를 부가가치 있는 정보로서 재생성하고 그것을 브라우징 능력이 뛰어난 웹 기술과 접목시키는 것이다. 지난 여러해 동안 데이터베이스 기술분야의 인기를 독점해온 관계형 데이터베이스(RDBMS)도 이러한 기능을 제공하기에는 역 부족이었다.

이를 해결하기 위해 새로운 데이터베이스 모델이 필요하게 되었으며 이러한 새로운 요구에 부응하여 개발된 것이 다차원(Multi-dimensional) 데이터베이스와 OLAP(OnLine Analytical Processing)으로 알려져 있다.

한편, 객체기술(Object Oriented)을 채용한 데이터베이스 업체들도 웹의 이러한 움직임에 대해 자체적인 기능 지원책을 강화하고 있다.

CGI를 이용한 데이터베이스 설계와 웹 인터베이스 구현

웹브라우저를 사용해 서버에 있는 데이터베이스의 정보를 보기 위한 인트라네트 애플리케이션(Application)을 개발하기 위해서는 CGI를 이용하여야 한다. 서버의 데이터베이스와 CGI의 인터페이스E를 위한 기본 기술로 플리 컴파일러(예,ORACLE의 PRO*C, Informix의 ESQL/C)와 RDBMS의 표준언어인 SQL, 4GL(예,ORACLE의 PL/SQL Informix의 informix/4GL)등 여러가지 언어를 습득해야 한다.

데이터베이스 차세대 언어인 SQL의 확장기능이며 절차적 기능과 온라인 트랜잭션 기능을 제공하는 SQL만을 이용해 인트라네트 애플리케이션을 개발 할 수는 있으나 완벽하게 구현할 수 없을 가능성이 많은 것이다.

데이터베이스의 저장 프로시져를 데이터베이스내에 저장시켜 놓아 웹브라우저 상에서 URL 혹은 IP 어드레스를 (예,http://www.chosun.com) 호출하면 웹의 특정한 기능이의 요청을 받아 데이터베이스의 특정 사용자로 접속해 이미 저장된 처리 과정을 거쳐 실행시킨다.

그 결과 자동적으로 HTML을 생성해 클라이언트 웹 브라우저 상으로 결과를 다차원 형태의 데이터타입으로 구성 즉시 내보내는 기능이 수행되는 것이다.

데이터베이스 문서의 HTML 문서로의 자동 변환

일반적인 데이터베이스에는 데이터가 테이블(table)라는 형태로 저장되어 있다. 이러한 형태의 데이터를 웹검색기 상으로 보기 위해는 HTML의 TR과 TD라고 하는 TAG를 사용 테이블의 로우(ROW)와 컬럼(COLUMN)이 많을 경우에는 상당히 많은 TR과 TD 태그로 TML은 자동 구성되며 상당히 복잡한 구조를 띄게된다.

이러한 전형적인 테이블을 쉽게보기 위해 인트라네트 개발 툴킷에는 여러 가지 다양한 유틸리티가 제공된다. 프로시저를 URL로 호출하면 결과적으로 웹검색기의 데이터베이스내의 테이블의 내용을 브라우저 캐쉬에 보관하여 보여준다.

데이터베이스의 정보를 웹상에서 보고자 할 때 전혀 CGI(Common Gateway Interface)를 사용하지 않고 쉽게 결과를 볼수 있도록 해준다.

프로시저를 데이터베이스내에 파저(PARSER) 형태로 저장시켜 놓고 웹브라우저의 URL에 요청으로 저장프로시져가 실행 되는데 그 결과는 CGI에서의 변수를 가진 다음 문서를 호출할 때 보통(예: HTTP://hostname/cgi-bin/HR-QUERY&the-

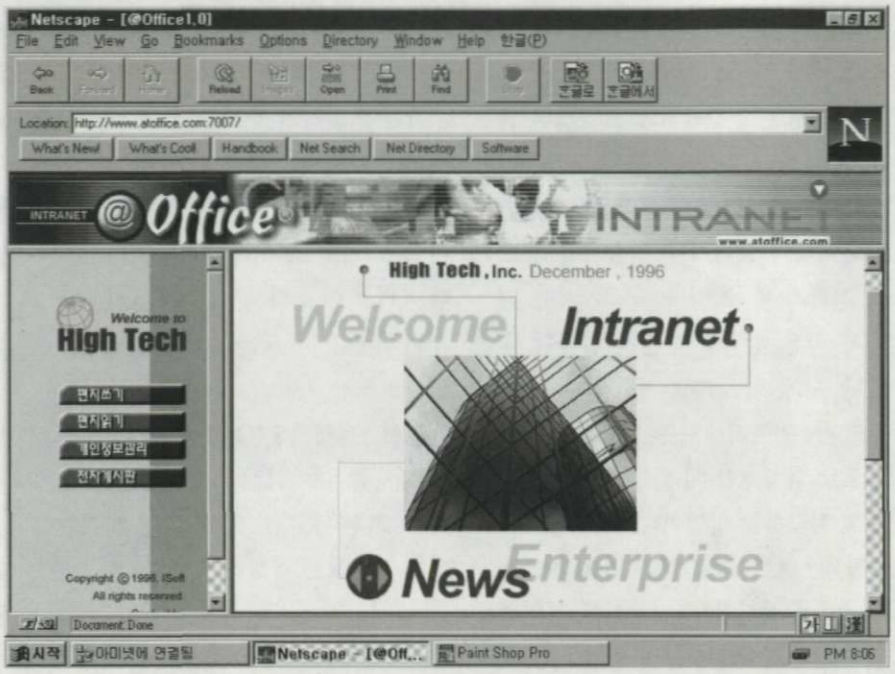
deptno 수)로 표현된다.

이러한 CGI 호출 방법의 단점은 인트라네트 환경에서 가장 중요한 보안사항이 외부로 공개 된다는 점이다.

즉 URL내에 비밀이 보장돼야 할 문서를 보기 위한 각종 변수가 화면에 표시된다는 점이다. 이것의 해결방안으로 저장 프로시져를 사용하면 호출할 때 조건을 위한 변수가 화면상에 표시되지 않고 내부프로시져에서 호출에 대한 변수가 내부적으로 옮겨지기 때문에 외부로 전혀 변수가 유출 되지 않는다.

한편 만약 웹브라우저를 통한 데이터베이스 액세스시 모든 쿼리(Query)가 로그인을 필요로 한다면 데이터베이스 서버에 걸리는 하중이 너무 커지게 되며 결국 그 영향이 사용자에게 까지 미치게 된다는 점을 유의해야한다.

이밖에도 데이터 서버로부터 데이터 소스까지의 연결에 대한 관계나 웹브라우저로부터 모든 사용자의 요구를 추적하는 작업이 필요하게 된다.



인트라 데이터웨어 하우스

데이터웨어 하우스의 정의

하드웨어나 소프트웨어 혹은 하드웨어와 소프트웨어의 중간인 펌웨어(Firmware) 처럼 데이터웨어(Dataware)라는 용어가 있다. 이 데이터웨어란 데이터자체에 부가가치를 부여해 데이터정보의 가치란 마치 소프트웨어 가치를 정히 측정할 수 없듯이 데이터 또한 가치를 정확히 평가하기 힘들다.

데이터 웨어하우스의 정의는 "기업의 운영목적 보다 관리자측의 의사결정 지원을 위해 설계된 주제지향적으로 통합가능하고 시계열적이고 영구적인 데이터의 집합"이라고 한다. 데이터 웨어하우스 주요 특성을 살펴보면 다음과 같다.

주제지향적 통합: 주제별로 데이터를 재구축 하기 위해 기업내 산재 되어 있는 각 부서들의 자료(Data)를 통합해야 한다.

예를 들어, 제품을 주제로 하는 데이터베이스는 매출액, 재고수준, A/S 요청 등 제품에 관한 모든 정보를 포함해야 하며 이를 위한 트랜잭션 데이터베이스에는 주문, 재고, 고객 등의 데이터베이스 테이블에 흩어져 있을 정보의 재통합(Reunion)을 의미한다.

시계열적 통합: 데이터는 일, 주일, 월, 분기, 반기, 연도 등 일정 기간 시간의 단위로 구분 요약된다 이렇게 요약된 데이터로 요일별, 계절별 등 기간 단위에 대한 기초 데이터를 입력함으로써 서로 비교 분석할 수 있는 기능이 있다.

영구적인 통합 : 기존 트랜잭션 데이터베이스와는 기본적으로 다른 목적을 위해 원시 데이터베이스로 부터 데이터를 추출/변형해 구축된다.

그러므로 사용자가 이것을 임의되로 직접 수정할 수 없도록 되어 있다. (예, 수익/지출 결산 마스터 DB등)

데이터 웨어하우스와 인트라네트

인트라네트에서 가장 부가가치 있는 정보 유통은 데이터 웨어하우스를 통해서 창출된다. 우선 데이터 웨어하우스를 웹에 연결하고 인트라네트에서 얻어지는 여러가지 장점으로는 첫째, 반복적인 데이터의 처리를 분석을 통해 절대적으로 시간을 단축시켜 주는 역할과 둘째로, 순간 사고나 분석에 의해 야기되는 유용한 부분 즉, 결과를 바로 볼 수 있는 데이터로 저장 가능하다는 것 세번째로 클라이

언트 서버 OLAP이나 레포팅 툴에는 포함되어 있지 않은 비동기처리(Asynchronous Processing), 데이터 압축(Data Compression), 데이터의 암부호화(Data Encryption)가 자유롭다는 것이다.

네 번째로 시간과 공간을 초월해 거대한 조직의 의사결정 지원 시스템에 정보를 활용할 수 있다는 점이다.

다섯번째로는 사용자 계층별로 별도의 추가의 네트워크의 설치가 필요없다는 점이다.

지금까지 살펴본 바와 같이 웹을 사용함으로써 기존의 클라이언트/서버 구조에 비해 잇점을 얻을 수 있다는 것은 의심의 여지가 없으나 웹 엑세스시 해결해야 할 문제들이 많이 남아 있다 역시 가장 중요한 것이 보안 문제이다.

웹검색기를 통한 데이터베이스 엑세스시 모든 질의가 로그인 프로시져로 연결한다면 데이터베이스 서버에 걸리는 하중이 너무 커져 결국 그 영향이 사용자까지 미치게 된다는 것이다.

인트라네트와 보안대책

인트라네트 방화벽

인트라네트를 구축하기 위해서는 보안 시스템을 어떻게 도입해 응용할 것인가에 대한 검토가 먼저 이루어져야 한다. 우선 인트라네트가 도입되기 전후의 네트워크 구조에 대한 위험적 요인 분석이 필요하다.

즉 네트워크에 연결된 모든 클라이언트, 호스트, 근거리네트워크, 리모트 네트워크가 운영되는 장비의 기능과 역할에 따른 체계적인 정보 수집과 시스템의 안전도가 어느 정도 수준인지를 분석해야 한다. 이것을 파이어월을 도입해야 한다.

이것의 순서로는 1) 대상의 선정 및 보안기준 설정 2) 네트워크의 분석을 토대로한 네트워크상의 헛점(Hole)이 되는 포인트를 체크하고 3) 네트워크 구성상에 필요한 요소에 적절한 불안요소 대상의 선정과 보안 기준을 수립한후 4) 어떠한 보안 시스템을 구축할 것인 가의 대한 설정이 필요하다.

즉, 공개되는 서비스 시스템의 엑세스를 제어하는 애플리케이션 서비스 및 사용자(User)의 대상 등을 지정해 필요한 보안 규칙을 정의하고 내부사용자 들도 특정한 호스트나 네트워크의 대한 접근을 제한할 필요가 있는지 면밀히 분석해야 한다.

보안이란 포괄적인 의미의 개념인데 그중에서 인트라네트를 구축할 경우에 보안은 크게 네트워크 보안, 시스템 보안, 데이터 보안 등으로 나눌 수 있다.

네트워크 보안은 네트워크를 보호하는 개념으로 일반적으로 파이어월이라 하는데 기능이 점점 추가되어 위의 3가지 보안기능을 부분적으로 지원하는 파이어월도 최근 소개되고 있다.

인트라네트의 보안 방식으로는 패킷검증 방식(Packet Filtering) 과 응용프로그램 게이트웨이 방식(Appli-cation Gateway)으로 크게 나누어진다.

최근에는 이 두가지가 혼합된 형태로 발전한 하이브리드(Hybrid) 방식과 서킷 레벨 게이트웨이 방식으로 발달되고 있다.

인트라네트를 위한 2가지 보안처리 이론

패킷필터링방식은 IP 어드레스와 포트 번호에 의해 접근을 제어하는 방식으로 주로 통신장비인 라우터 수준에서 해결지원이 된다.

애플리케이션 레벨 게이트웨이 방식은 프락시(Proxy)를 이용해 외부에서 내부로 접근을 지원하는 방식으로 외부와 내부를 완벽하게 차단할 수가 있다. 상위 레벨의 보완 기능을 지원하기 위해서는 이 방법을 사용하는 것이 좋다.

응용프로그램 게이트웨이방식은 최근의 해킹 사고의 70%이상이 내부사용자의 소행으로 증가하므로 특별한 기능의 애플리케이션이나 정보를 지닌 시스템에 접근을 제어하는 방식으로 파이어월은 주로 네트워크 보완에 치중하기 때문에 시스템 보완의 측면이 매우 취약할 수 도 있으므로 파이어월을 도입시 이 부분도 함께 고려할 요소라 생각된다.

자료보안은 국내외적으로 가장 이슈가 많이되고 있는 보안 항목중 하나로 네트워크간의 데이터를 주고 받는 경우 데이터를 암호화 전송하는 방식이다.

암호화 알고리즘은 RSA, DES 등을 기본으로 한 제품들이 대부분이며 최근 국외에서 RSA는 자국의 이익보호 차원에서 수출이 금지된 것으로 알고 있다.

인트라네트 보안성 및 구축체계

보안 제품마다 지원하는 기능에 차이가 있기 때문에 사용자 사이트에서 필요한 기능을 지원할 수 있는지를 검토해야 할 것이다.

즉 그룹웨어, 워크플로우 등의 업무를 지원하는 클라이언트 서버 모델의 애플리케이션으로 지원 가능한 IP 어드레스를 지원해주는 주소 변환기능, 파이어월 제품의 리모트 메니지먼트 기능 등이 가능한가 하는 점을 각자의 시스템에 맞게 적용할 수 있는가를 검토할 필요가 있다.

보안제품에도 일부는 애플리케이션의 지원이 불가능한 제품도 있다는 것을 반드시 알아둘 필요가 있다. 왜냐하면 보안제품이라고 사용자가 원하는 모든기능을 지원하는 것은 결코 아니기 때문이다.

보안에 대해 투자의 범위를 결정하드라도 보안시스템을 구축하려면 네트워크 환경설정의 설계가 선행돼야 한다.

기존의 서비스의 위치 이동이 있을 수도 있고 새로운 시스템에 수요가 발생할수도 있기 때문에 투자 및 예산의 범위가 정해지면 인터네트와 인트라네트의 네트워크의 기술이 빠르기 때문에 설계가 필요하다.

앞으로의 보안제품도 신기술의 대응 빠르게 적용할 수 있는 것이어야 한다는 것이다. 또한 중요한 사안으로 반드시 유지보수 부분을 포함해야 한다.

유지보수가 중요한 이유는 파이어월이 새로운 아키텍처의 프로토콜이나 애플리케이션이 개발되면 이에 대응하는 파이어월의 해결책(Solution)의 지원이 빠른 파이어월을 선정해야 하기 때문이다.

그다음이 퍼포먼스 영향이다. 대부분의 업체에서 가장 민감한 부분으로 실제로 파이어월을 설치하였을 경우 일부 제품들은 퍼포먼스가 높아지거나 낮아져 어렵게 되는 경우도 있다.

1995년 11월 IDC 사에서 벤치 마크 테스트한 자료가 있는데 20여개사의 파이어월 제품의 비교자료로서 여러개의 항목을 정해 실시했다.

가장 중요한 점은 파이어월을 설치할 때 전산망 전체에 대한 퍼포먼스에 영향을 최소화할 수 있도록 해야 한다는 점이다.

일부 제품들이 클라이언트의 접속수의 따라서 퍼포먼스가 현저히 차이가 나는 제품이 대부분이고 심지어는 클라이언트 접속 노드가 많아지면 파이어월의 기능을 지원하지 않는 제품도 일부가 있다.

기업의 네트워크환경이 초고속망의 구축단계로 발전하고 있으므로 파이어월이 지원하는 네트워크 퍼포먼스도 고려해야 한다.

파이어월이 10Mbps 이더네트만을 지원하는 경우도 있으므로 자사의 네트워크 백본이 FDDI, ATM등으로 구현될 경우를 대비해 파이어월을 선정하는 것이 중요한 문제이다.

파이어월(방화벽) 시스템 설치

보안제품 선정이 끝나게 되면 보안시스템을 설치하는데 우선 보안업체 담당자를 통해 네트워크 환경설정을 분석해 보안시스템을 두어야 할 네트워크상의 포지션을 지정, 어떤 보안정책을 적용하고 어느 부분의 취약점을 가지고 있고 보안시스템을 적용할 경우의 보안 대책은 어떤 방법으로 이루어지는지를 체크한다. 이런 분석작업이 끝나면 그 결과를 가지고 이루어진다.

이를 각 단계별로 알아보면 1 단계에서는 전체적인 보안 설계를 하는 단계로서 네트워크 분석 결과를 갖고 다시 기존의 네트워크를 재구성하는 과정이 수반되는 과정으로 주로 내부의 터미널 서버, 시스템의 접속된 다이얼 업 모뎀, WAN 구성을 위한 내부 라우터 등을 외부의 연결노드로 접속을 바꾸어야 하며, 일부 공공 서비스의 목적으로 지원되는 시스템 등도 이단계에서 검토 대상이 된다.

인트라네트 보안시스템 설치단계

1 단계: 전체적인 보안 설계
2 단계: 외부망과의 물리적 연결점의 보안
3 단계: 패킷 필터
4 단계: 응용보안 게이트웨이 설치
5 단계: 서브넷사이의 보안
6 단계: 호스트 보안
7 단계: 보안 인지도 교육과 같은 설치 작업

2 단계에서는 외부망과의 물리적 연결점의 보안으로 전용회선의 연결(DSU, CSU)이나 다이얼 업 서비스(모뎀)가 있을 경우 일부업체는 전용회선이나 전화선이 노출되어 있는지 등을 검토하는 단계이며, 3단계는 패킷필터링단계로 주로 라우터 수 내부에서 지원되는 기능으로 엑세스 리스트를 만들어 필터링 기능을 활용함으로써 네트워크의 정보의 유출을 사전에 방지한다든지 접근하고자 하는 네트워크를 제한하는 기능을 제공하는 것이다.

최근에는 라우터 장비들의 보안기능이 많이 강화되는 추세이다. 그러나 일부 네트워크 관리자들중 라우터만을 가지고 파이어월 기능을 지원한다고 해 파이어월은 필요없다고 착각하는데 이는 라우터의 정확한 개념을 미리 파악하는 것이 필요한 경우이다.

보안 관리자는 라우터에 대한 별도의 장비 이력관리지를 만들어 랜, WAN 포트에 대한 패스워드, 엑세스 리스트 관리 내용을 기록해 정리한다. 패스워드는 특별히 주의해 운영하도록 한다.

일부 네트워크만을 전문적으로 하는 업체중 라우터를 관리하는 경우 모든 포트에 대해 동일한 패스워드를 적용해 사용하는 업체도 있는데 보안 측면에서 배제돼야 할 필수상황이며 해당 업체에서 별도로 관리하는 것을 추천하고 싶다.

4단계는 응용보안 게이트웨이 설치하는 부분인데 일반적으로 파이어월을 설치한다는 것은 이 단계에서 실시된다. 파이어월이 설치되기 전에 파이어월 머신이 네트워크 환경설정에 정확히 정의 되었는지 체크한다.

대부분의 파이어월 설치 시간이 가장 많이 소유되는 시점이기도 하며 모든 문제의 근원이 될수도 있다. 어드레스 변환기능을 지원하는 파이어월을 사용하면 내부 사용자의 어드레스가 부족한 점을 지원하고 내부 어드레스 정보의 노출을 피할수 있다.

RFC1918에서 권고하는 프리바이트 인터네트 어드레스를 사용할 수 있는 어드레스가 있는데 이것은 표 2와 같다.

〈표 2〉 프리바이트 인터네트 어드레스

변경전 IP Address	변경후 IP Address
10. 0. 0. 0	10.255.255.255
172. 16. 0. 0	172.31.255.255
192.168 .0. 0	192.168.255.255

이처럼 지정된 어드레스는 일반 유저 사이트에서 임의로 지정해 사용할 때 이용가능한 영역으로서 다른 어드레스를 지정해 쓸 결우에는 그 어드레스를 실제로 할당받은 사용자와 통신할 때 충돌 문제가 발생되므로 정상적인 사용이 안된다. 표 2의 정의된 어드레스는 라우터에서 라우팅 정보가 교환이 되지 않고 인터네트를 통해 공인 어드레스로도 할당 되지 않는 어드레스이다.

5단계는 서브넷사이의 보안으로서 주로 본사와 지사처럼 WAN으로 구축된 네트워크와의 연결시 서부네트워크와 본사의 양쪽에 파이어월을 설치해 보안을 구축하는 것이다. 대부분의 파이어월을 설치하는 업체의 경우에 WAN으로 구축된 네트워크는 주로 내부의 사용자이기 때문에 안전하다고 판단하는데 사실 이런 경우가 가장 위험한 요소라고 할 수 있다.

일반적으로 파이어월을 설치하였다고 무조건 안전하다는 생각을 가지는 것은 대부분의 파이어월 구매업체들의 생각이다. 그러나 이는 잘못된 생각인데, 최근의 해킹 시도의 70%이상이 내부 사용자의 소행인 점을 감안한다면 내부 사용자의 대한 보이지 않는 보안의 측면도 강화해야 한다는 것이다.

특정한 정보를 제공하는 머신이나 유저의 퍼미션을 체크해 호스트에 불필요한 사용자 개정을 체크해 삭제하도록하고 주기적으로 ID에대해서도 패스워드를 변경하는 작업을 실시하며, 시스템의 사용되는 파일의 스티키 비트를 체크해 불필요한 파일은 삭제하도록 한다. 매일서버 같은 경우에는 항상 최신 버전을 사용하도록 하고 호스트(hosts) 파일에서 리모트 호스트를 정의할 경우 리드/라이트 퍼미션, 유저, 호스트 등을 정의해 기록야 할 것이다.

보안에 관련된 패스를 체크해 설치하는 작업도 중요하다. 즉 패치 설치 리스트를 관리해 최신 버전의 패치를 설치하는 것도 필요하다.

7단계는 보안인지도 교육에대한 부분인데 파이어월이 설치가 6단계과정을 거쳐서 정확히 설치 되더라도 보안 정책에 의해 지속적으로 운영이나 관리가 중요하며 철저한 관리체계가 이루어져야 한다. 이와같은 과정을 거쳐 파이어월의 설치가 비로소 완료된다.

지금까지 인트라네트의 구축방법과 구현기술 인트라네트를 이용할 때 필수적으로 고려하여야 하는 통신 보안 환경 등에 대해 살펴 보았다 결과적으로 인트라네트를 조직내에서 성공적으로 구축하기 위해서는 기존 컴퓨터환경과 새로운 기술의 접목이 절실하다.

다양한 기술을 구현하기 위한 각종 개발툴과 개발언어 그리고 새로운 형태의 데이터베이스 구축 등을 이해하고 사용해야만 하는 것은 아니다. 자사 환경에 맞고 경제적인 인트라네트를 구축해야한다는 점이다.

즉, 자사 개발인력이나 관련조직이 혼연일체가 될 수 있도록 사전에 면밀히 계획을 수립 검토한 후에 추진하는 것이 효과적일 것이다.

결과적으로 말해 인트라네트를 잘 구축한다는 것은 기업이 새로운 정보 시스템의 흐름에 능동적으로 대처할 수 있는 기업의 컴퓨팅 즉, 새로운 형태의 정보 시스템을 완성하는 일인 것이다.