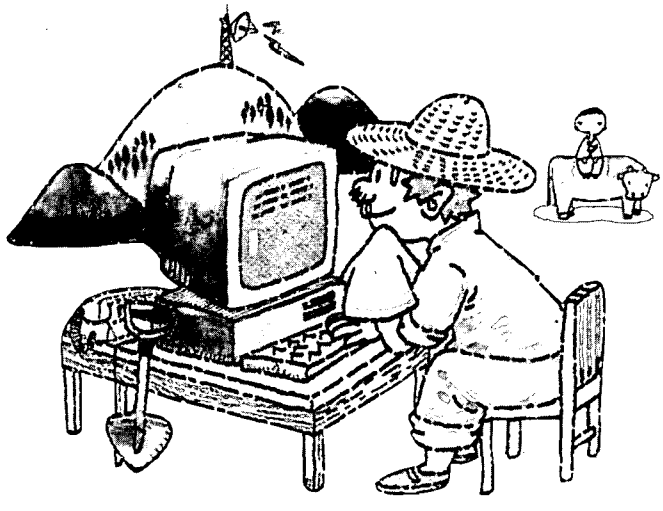
데이터베이스와 해커(Ⅳ)

(Database & Hacker)

한상근
한국과학기술원 수학과 교수
Han, sang-geun. / Korea Advanced Institute of Science and Technology.



4. 해커의 미래 - Cypherpunks의 등장

요즘에는 가상현실이나 사이버 스페이스등의 새로운 단어가 신문이나 잡지에 자주 나오고 있다. 사이버펑크(Cyberpunks)라는 단어도 자주 나오는데, 사이퍼펑크(Cypherpunks)는 사이버펑크와는 다른 뜻을 가지고 있다. 사이버펑크의 등장은 현재의 인간이 컴퓨터를 사용해서 만들어낼 미래의 세계에 대한 희망, 동경심, 불안감, 증오감등을 기초로하는 일종의 문화현상이다. 말하자면 한때 공상과학 소설이나 공상과학 영화가 엄청난 유행이었던 것처럼, 지금의 사이버펑크는 미래 정보사회의 중요한 도구가 될 컴퓨터와 그 컴퓨터를 사용하게될 미래의 인간들에 관한 지금 사람들의 호기심과 상상력이 만들어낸, 21세기 정보시대로 변해가는 과정에서 나타나는 유행을 따르는 사람들을 말한다. 사이퍼펑크에 대해서 이야기하려면 우선 현대 암호학에 대해서 말하지 않을수 없다. 암호(Cypher, 암호학은 영어로 Cryptology다.)라면 대개는 간첩이 몰래 감추고있는 난수표를 생각하는데, 1980년대 초까지

는 암호에 대해서 갖는 일반인의 그런 생각이 실제상황과 별로 다름이 없었다. 그러나 그 이후에 나온 공개열쇠(Public Key) 암호는 그런 일반인의 상식을 송두리째 바꾸어 놓았다. 옛날의 암호에서는 암호문을 보내는 사람과 암호문을 받는 사람이 두사람만 아는 똑같은 비밀 패스워드를 사용해서 암호문을 해독했다. 즉 암호문을 받는 사람과 보내는 사람이 비밀 패스워드라는 두사람만의 비밀 정보를 공유해야만 했다. 그러나 필자의 연구분야인 정수론이 발달하자 전혀 새로운 공개열쇠 암호체계가 만들어졌다. 이방식을 간단하게 말하자면 필자(암호문을 받는 사람)가 혼자서만 비밀 패스워드를 만들어서 아무에게도 알려주지 않고 혼자서만 알고있어도 된다. 문장을 암호문으로 바꾸어서 보내는 사람은 필자만 알고있는 이 비밀 패스워드를 몰라도 암호문을 만들수 있다. 그이유는 필자에게 암호문을 보내려고 하는 사람은 필자만 알고있는 비밀 패스워드를 모르더라도, 문장을 암호문으로 바꿀수 있도록 바꾸는 방법은 필자가 공개하기 때문이다. 즉 누구라도 필자에게 암호문을 보낼수는 있지만 암호문을 해독하는것은 필자만이 할 수 있다는 것이다. 이 공개열쇠 암호는 인터넷에서 컴퓨터끼리 서로 확인해보는데 사용되기도 하고, 요즘에 많이 거론되는 스마트카드에 사용되는 암호체계이다. 미국의 산업 및 응용수학회(Siam)에서 회원 명부를 관리하는데에도 이 공개열쇠 암호를 사용한다. 회원명부는 암호문으로 바뀌어져서 보관되어 있으며, 어느 회원이라도 자기자신에 관한 정보는 그때그때 고치거나 새로 입력할수 있다. 다른 사람을 찾아보고 싶을 때에도 그사람의 이름등을 가지고 연락처나 전화번호등을 찾아볼수 있는데, 다만 광고문을 돌리기 위해서 회원명단 전체를 읽어보는 것은 회원 전부를 이미 알고있기 전에는 불가능하다.

워드프로세서등에도 암호기능이 들어있는 상품이 있는데, 대개의 상품에 사용되는 암호는 그 안전성이 대단히 취약한 것들이다. 민간회사가 사용하는 암호기술의 수준과 미국이나 러시아같은 강대국의 정보기관이 사용하는 암호기술의 수준은 하늘과 땅 차이다. 미국 정부가 1970년대에 연방 표준으로 승인해서, UNIX에 로그인하는 과정에 사용되는 DES(Data Encryption Standard)만해도 민간 회사에서 1990년대의 첨단 워드프로세서에 사용하는 암호들과는 비교도 할수 없을만큼 고급 암호이다. 그 이유는 워드프로세서에 암호기능을 넣을 때에 암호론을

공부한 사람이 전혀 참여하지 않고 전산학을 공부한 프로그래머들이 일을 다 하기 때문이다. 한글과 컴퓨터社의 워드프로세서에 사용하는 암호를 해독할수 있는 프로그램을 누군가 만들어서 무료로 배포했는데, 외국에는 "암호를 잊어버려서 애써 작성한 귀중한 자료를 사용하지 못하는 분들을 위해서" 잊어버린 암호를 찾아주는 프로그램이 많이 있다. 그런 상품을 판매하는 회사에서 부르는 값은 보통 일이백불 정도이

다. 이 암호 찾아주는 프로그램의 피해를 가장 심하게 당한 회사는 아마도 압축 프로그램인 PKZIP을 만드는 회사일 것이다. PKZIP의 암호가 안전하지 않다는 소문이 계속해서 나오자, 이 회사는 지난해에 상금을 걸고 자기 회사의 암호를 풀어보라고 했으나 여러 사람들이 순식간에 풀어냈다. 공개열쇠 암호체계가 중요한 또 다른 이유는 이 암호가 정보기관이나 군대에서 나오지 않고 민간인들이 독자적으로 찾아낸 최초의 암호이고, 수학적으로 그 안전성(혹은 불안전성)에 대해서 어느 정도 구체적으로 예상할 수 있기 때문이다. 고전적인 암호체계에서는 그 안전성은 대부분 경험에 크게 의존해서 판단한다. 즉 정보기관이나 군대에서 그전에는 모르고 있던 암호체계를 민간인들이 만들어냈고, 이 암호체계가 대단히 좋아보인다는 것이다. 게다가 사용자는 비밀 패스워드를 누구에게도 알려줄 필요가 없다. 만일 이것이 전세계적으로 쓰인다면 모든사람이 통신에 있어서는 완벽한 프라이버시를 가질 수 있게된다. 그리고 여기에서부터 국가 권력과 개인의 자유사이의 대충돌이 일어나게 된다. 미국의 국가안보국(NSA)은 인터넷을 자동감시하는 프로그램을 가지고 있는데, 사람들이 메세지를 암호문으로 바꾸어서 전송하면 도청에 성공하더라도 암호문을 해독하기 전까지는 아무런 효과가 없다. 지난해에는 미국에서 일단의 해커들이 인터넷으로 지나다니는 패스워드를 수백만개나 가로채가서 사용자 모두에게 패스워드를 바꾸라는 권고가 신문에 난적도 있었다. 대개의 통신 프로토콜에서는 데이터가 암호문으로 바뀐 상태로 돌아다니지 않기 때문에 통신회선을 도청해도 패스워드를 알아낼수 있다. 로그인하는 과정을 암호문으로 바뀐 상태에서 하는 몇가지 통신 프로토콜이 있는데, 아직은 사용하는 사람이 많지않다.

사이퍼펑크란 강력한(초강대국의 정보기관도 백년이내에는 도저히 해독할수 없는 대단히 안전한) 공개열쇠 암호를 누구나 마음대로 사용할수 있어야 된다고 굳게 믿는 사람들이라고 생각하면 틀림없다. 이들은 지금 당장 사용가능한 기술로 모든 사람에게 완전한 프라이버시자유를 줄수있는데, 만일 이것을 정부나 거대기관이 마음대로 통제하게 놓아두면 공상 과학소설 1984년에 나오는 전체주의 국가가 된다고 믿는다. 사람들에게 완벽한 프라이버시를 주는 댓가로 범죄의 수사가 대단히 어려워지거나 국가, 거대기관이 미미한 존재로 바뀌고 혹시 전세계가 무정부상태까지 가는 일이 발생하더라도, 그것은 국가의 소멸을 통한 새로운 시대의 도래일 따름이라고 생각한다. 본격적인 수준의 사이퍼펑크는 전 세계에 100명 이내로 추산되는데 1992년 가을무렵부터 나타난 이들은 구체적인 조직체를 가지고 있지는 않으나 서로가 유기적인 협력관계를 가지고 있으며 작년부터는 샌프란시스코나 뉴욕등지에서 지역별 모임을 가지고 있다. Toad.Com을 통해서 메일을 받아보는 사람의 수는 칠백명 정도이고, 그 대부분은 해커들처럼 젊은 학생들이다. 필자도 기회가 되면 이들의 모임에 한번 참가해볼 생각이다. 이들이 스스로 밝힌 견해는 다음과 같다.

"사이퍼펑크의 생각으로는 프라이버시는 중요하며, 사람들은 조금이라도 프라이버시를 더 가지기 위해서 수백년을 노력해왔다. 프라이버시는 사람들이 가만히 있으면 정부나 거대기관이 거저 갖다주는 것이 아니다. 프라이버시를 지키는 가장 중요한 방법은 암호를 사용하는 것이다. 원하는 사람은 누구라도 강력한 암호를 사용할 권리가 있다. 우리는 원하는 누구에게라도 암호를 사용하는 방법을 가르쳐줄 생각이다. 우리는 이를 위해서 암호를 연구하고, 제작하고,

실험한다."

사이퍼펑크의 주장에 대해서 "그것은 당연하지 않은가 ?" 아니면 "그렇게 해서는 안된다." 라고 생각할 사람들이 있을 것이다. 그런 생각은 사이퍼펑크가 주장하는대로 누구나 강력한 공개열쇠 암호를 사용하는 세상은 어떤 세상이 되는지 추측해보면 이 문제가 그렇게 단순한 문제가 아니라는 것을 알게된다. 사이퍼펑크의 한 사람이라고 볼수있는 필립 짐머만은 PGP라는 암호 프로그램을 무료로 배포했다. 그런데 캘리포나아에서 어느 마약 밀매업자가 잡혔는데, 이 범죄자는 자신의 마약거래기록을 PGP를 사용해서 암호로 만들어 보관하고 있었다. 미국 경찰은 짐머만에게 PGP의 해독을 요구했지만 짐머만은 자신도 해독은 할수 없다고 하며 이 요청을 거절했다. 암호 프로그램을 만든사람이 법원에서 발부한 영장을 이렇게 거절할수 있는지도 생각해볼 문제이지만, 중요한 문제는 이미 여기에 그 누구도 감히 해독해 볼 엄두도 못내는 암호체계가 있다는 데에 있다. 게다가 수학의 정수론은 그런 암호체계를 해독하는 것은 앞으로 몇백년뒤에나 겨우 가능하게 될지 모른다고, 해독하는 데에 걸리는 이론적인 최단시간을 추측하는 단계에 와있다. 모든 범죄자나 테러리스트들은 적어도 통신에 있어서는 완벽한 보안장치를 가질수 있는 단계에 와있다는 것이다. 멕시코의 Chiapas에서 활동중인 반군도 암호통신에 PGP를 사용한다는 보도가 있었다. 잘하면 도청이라는 단어는 경찰의 사전에서는 얼마 안가서 없어질지도 모른다. 미국의 클린턴 대통령은 범죄자들이 이토록 강력한 암호를 마음대로 사용하는데에 대한 대비책으로 민간인은 누구도 해독할수 없고, 다만 FBI만 도청해서 해독할수 있는 클리퍼(Clipper) 암호자재를 사용하자고 제안했으나 여러 인권단체의 거센 반대에 직면하고 있다. 인권단체가 보기에는 클린턴 대통령의 제안은 "우리는 너희들의 전화나 통신을 항상 읽어볼 테니까, 백성들은 안심하고 이 암호를 사용해라. 적어도 백성들끼리는 평등하다."와 똑같은 것이다. 위의 PGP와 같은 암호자재는 미국의 수출금지 품목에 무기로 분류되어서 들어있다. 짐머만은 수출이 금지된 PGP를 수출했다는 죄목으로 지금 재판받고 있으며 인권단체와 사이퍼펑크들은 짐머만의 변호사 비용을 모금중이다. 이 PGP를 가져다가 직접 써보고 싶은 사람은 필자에게 연락하면 된다. 사이퍼펑크는 클린턴 행정부가 클리퍼 암호를 제안하기 반년전에 이미 그런 암호의 위험성을 경고해서 일약 메스컴의 각광을 받았다.

변호사, 의사, 신부등은 직무중에 알게된 사실은 누구에게도 발설하지 않을 권리와 의무가 있다. 그런데 우체국이나 전화국은 편지나 전화를 보내는 사람과 받는 사람을 보호해야 하는 의무가 있을까? 만일 우체국이나 전화국에서 편지나 전화를 주고받는 사람들의 주소나 전화번호를 확실하게 지켜주면 유괴범들이 훨씬 더 많이 생겨날 것이다. 컴퓨터를 이용하여 무기명(Anonymous) E-Mail 재발송(Remailer) 서비스를 하는 사람들이 있다. E-Mail을 주고받는 사람들의 주소를 암호로 만들어놓고 암호문으로 바뀐 메세지를 중간에서 다시 암호문으로 바꾸어서 발송하는 일을 여러번하는 것이다. 이렇게하면 누구라도 서로의 신분을 완벽하게 감춘상태에서 통화할수도 있다. 일단의 사이퍼펑크들이 무기명 재발송을 이용하여 정보의 암시장(일명 Blacknet)을 시도하고 있다. 이 세상의 어떠한 정보라도 안전하게 사고팔 수 있는 이 암거래 시장은 지금은 미국의 FBI가 수사중이라고 한다. 무기명 재발송같은 좋지 않은 것은 금지해야 한다고 생각하는 사람이 있겠지만,

직불카드나 선불카드, 전화카드를 생각해보자. 어떤 사람이라도 그사람이 전화카드를 가지고 언제 어디에서 누구에게 전화를 하고, 어느 가게에서 어떤 물건을 얼마만큼 샀는지가 날마다 기록되어서, 누군가가 항상 그 기록을 읽어보고, 신용카드 회사나 은행에서는 때때로 신용이 좋지 않다고 대출해주지 않고, 경찰, 은행, 신용조사 회사나 컴퓨터 해커, 전산운영 요원이 그사람에 대해서 손바닥 들여다 보듯이 안다면 좋아할리 없다. 해커들은 가끔 자기네 해커에 대해서 좋지 않은 글을 쓰거나 하는 사람에게 보복할 때에, 그사람의 신용평가 기록을 엉망으로 바꾸기, 하루에도 수백통씩 전화가 잘못 걸려오게 만들기, 그사람의 전화로는 통화할수 없도록 하기, 그사람의 은행 구좌를 가지고 장난하기, 그사람의 신용카드 번호나 비밀번호를 공개하기, 지명수배자 명단에 그사람의 이름을 올려놓기, 도난신고 차량목록에 그 사람의 자동차 번호를 올려놓기, 공공기관에 보관되어 있는 가족사항이나 신상정보를 바꾸어 놓기, 장거리 전화를 할때에 전화요금이 그사람에게 청구되도록 공짜로 장거리 전화하는 방법을 공개하기등을 한다.

개개인에 대한 이런 정보의 남용은 러시아의 어느 소설가가 쓴 작품에 나오는, 미래세계에서는 섹스를 하고싶은 남녀는 사방이 투명한 유리로 만들어진, 길가에 있는 방에 같이 들어가서 자야한다는 내용을 생각나게 한다.

어느나라에서나 뇌물을 주고받을 때에는 현금을 사용하는데, 만일 모든 지폐의 번호가 컴퓨터에 기록되어 있고 온세계의 모든 사람들이 언제 어디에서 누구에게 얼마를 주었는지가 모두 기록된다면 어떤 세상이 될까? 유럽 연합에서는 디지털 현금을 추진중이고 우리나라의 조폐공사에서도 이를 연구중이다. 뇌물을 현금으로 받는 이유는 추적이 불가능하기 때문이다. 이런 이유로 십만원 짜리 자기앞 수표를 십만원 짜리 지폐로 바꾸는 것을 반대하는 사람들이 있다. 화폐는 결국에는 디지털 현금으로 바뀔 전망인데 지금 논의되는 각국의 디지털 현금은 모두 추적가능한 것만이 검토 대상이다. 세무서와 경찰서에서는 무척이나 좋아할 것이다. 사람들은 자기가 어떤 치약을 가게에서 사가는지가 데이터베이스에 들어가서 집으로 다른 회사의 치약 광고가 날아오는 사회를 원할까 ? 디지털 현금을 추적 불가능하게 만들면 부피도 없이 컴퓨터 내부에 데이터로 존재하는 디지털 현금은 이번에는 범죄 집단의 돈 세탁이나 살인 청부업자, 탈세, 뇌물, 도박등에 아주 유용하게 사용될 것이다. 온라인 뱅킹이나 홈 뱅킹, 인터넷에서 신용카드 번호를 이용한 상품구매는 이미 실용화되었으나 그 안전성을 의심하는 소비자의 반응이 아직은 냉담한 편이다.

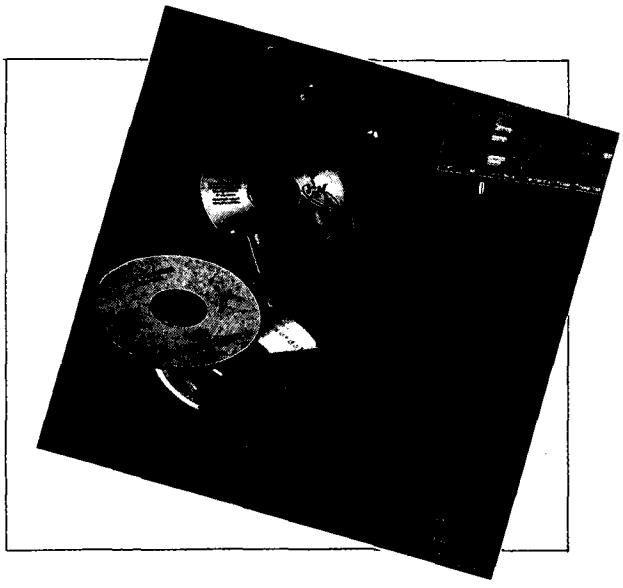
그 이유는 해커들이 한번 금융기관의 전산망에 침입하면 수천개의 신용카드 번호가 새나가기 때문이다. 따라서 이런 안전에 관한 소비자의 불안감을 줄이기 위해서도 이러한 거래는 필연적으로 공개열쇠 암호를 사용해서 암호화 될것이다. 그리고 이때에 사용되는 암호가 무기명성을 보장해주는가 아니면 모든 거래가 실명거래가 될 것인가, 무기명거래라면 거래가 이루어진 후에라도 수사기관의 추적이 가능한 암호를 사용할 것인가 아니면 추적이 원천적으로 불가능한 암호를 사용할 것인가에 따라서 미래 사회의 구조는 크게 달라질 것이다. 이 모든것은 현재의 우리가 깊이 생각해 보아야 할 문제들이다. 이 글을 읽는 누구라도 "추적 불가능하고 무기명"으로 되어야한다고 공감할 일이 하나 있는데 그것은 선거이다. 전자 선거를 하게되면 선거당일에 저녁을 들면서 결과를 알수있게 될것이다. DBC

급속히 발전하는 WWW와 MOSAIC

-효율좋은 정보검색이 과제로-

The Rapid Development of WWW(Word Wide Web) & Mosaic

최상희/조선일보 뉴미디어연구소
Choi, Sang-Hee,/Chosun Ilbo
Newmedia Institute



인터넷이라는 Cyberspace는 점점 확대되고 있으며,우리는 보다 많은 정보를 인터넷을 통하여 교환하고 있다. 여기서는 인터넷의 정보를 사냥하는 정보검색도구에 대하여 설명하며, 실제로 인터넷에 정보를 서비스할 경우에 어떻게 해야하는지를 설명하고 있다. 여기서 필자가 제안한 방법은 현재 상당부분이 이미 구현된 것도 있다.

(譯者註)

인터넷(Internet)정보서비스인 WWW(Word Wide Web)과 그 열람도구(Browsing Tool)인 모자이크 (Mosaic)이 급속하게 확산되고 있다. WWW는 하이퍼텍스트를 확장한 분산형 하이퍼미디어 시스템인데, 문자이외의 화상 및 음성 등을 전송할 수 있고, 기존의 인터넷 정보자원과도 결합하여 사용할 수 있다. 한편, WWW으로 제공되는 정보량이 늘어나면서, 필요한 정보를 찾기는 더 어려워지고 있다.따라서 모자이크에 지적인 인터페이스를 부가하여, 이용자의 흥미에 맞는 정보를 선별하는 것이 필요하다. 인터넷의 최신 정보서비스인 WWW(World Wide Web)은, 하이퍼텍스트링크(Hypertext Link)를 사용하여, 텍스트문서와 화일을 연결시킨다.

이 방법은 이용자가 하이라이트(Highlight)로 표시되어 있는 단어나 텍스트중의 구절

(phrase)을 링크하기만 하면, 선택한 어구에 관련되는 추가정보를 얻을 수 있다. 나아가 이용자는 하이퍼텍스트를 확장한 하이퍼미디어를 사용하여 도형, 이미지, 음성 및 Full Motion 동화상에서 접근(Access)할 수 있다.

WWW 프로젝트는 분산형 하이퍼미디어시스템을 구축하는 실험으로서 스위스의 CERN (European Center for Nuclear Research : 유럽핵물리학연구소)에서 시작되었다. 이용자는 브라우저 프로그램(Browser Program)을 통하여 WWW에 접속하여 문서를 읽기도 하고 얻기도 할수있다. 자기의 컴퓨터가 접속되어 있는 LAN상의 문서만이 아니라, 인터넷을 경유하여 세계 컴퓨터에 있는 문서를 얻을 수 있다. 부라우저는 FTP 및 NNTP, Gopher등의 인터넷 프로토콜을 사용하여, 화일에 접속한다. 원격지에 있는 상대방의 서버에 접속가능한 기능이 있으면, 클라이언트의 브라우저는 문서 및 데이터베이스를 검색할수 있다

모자이크가 가장 인기가 좋다.

브라우저는 종래의 단말기에서 사용하는 코맨드라인 형식이라도, 최근의 그래픽표시 단말의 그래픽형식이라도 좋다. 그래픽형식의 브라우저로 가장 인기있는 것이 모자이크이다. 이 모자이크은 GUI (Graphic User Interface)에서 WWW을 이용하는 수단으로 미국 NCSA (National Center for Supercomputing Applications)가 개발하였다.

NCSA의 WWW 브라우저의 최초버전은 X-Mosaic이라고 불리는데, UNIX의 X-Window시스템용 WWW 클라이언트이며 인터넷에 공개된 것은 1993년말이다. GUI가 사용하기 쉽기 때문에 X-Mosaic는 WWW용 인터페이스로 가장 많이 보급되었다.

모자이크은 비동기방식으로 협조처리를 하는 광역분산시스템이며, 하이퍼미디어를 사용하여 정보의 탐색 및 검색이 가능하다. X-Mosaic브라우저는 X-Window시스템이 작동하는 Unix 워크스테이션 및 MS-Windows가 작동하는 PC; 또는 매킨토시에서 이용가능하다.

모자이크은 WWW Server 이외에 WAIS (Wide Area Information Servers), Gopher Server, Archie Server 등에 있는 데이터에도 접근가능하다.

모자이크는 기능이 충실하다.

모자이크에는 편리한 기능이 많이 있기 때문에, 많은 영리기업 및 정부기관,대학 등이 모자이크로 이행하고 있다. 모자이크는 일관되게 마우스를 사용하여 조작하는 그래픽 인터페이스를 가지고 있다. 디지털데이터를 다양한 폰트 및 스타일로 표시할 수 있다.

모자이크는 SGML(Standard Markup Language)과 HTML(Hyper Text Markup Language)로 기술된 텍스트를 읽어들여서,보기 좋게 정리한 정보로 표현할 수 있다. 모자이크는 또 필드, 체크박스, 라디오버튼이라는 기본적인 표시요소를 취급한다. 불어, 독어, 하와이어 등의 IS08859표준으로 규정된 각종언어의 문자도 표시할 수 있다. 나아가, 256color의 그래픽(GIF형식 및 X-Bitmap형식), 디지탈오디오 및 디지탈비디오에도 대응가능하다. 이용자는 모자이크의 기능을 확장할 수 있다. Custom Server를 만들어서 다른 어플리케이션으로 화면표시를 원격조작할 수 있다.

예를 들자면, NCSA의 DTM(Data Transfer Mechanism)을 사용한 Collage같은 멀티

프랫폼용 그룹웨어를 이용하여, 모자이크 화면 내용을 이용자에게 브로드캐스트(Broadcast)할 수 있다.

모자이크 이용자는 하이퍼링크를 통하여 기본적인 네트워크 서비스(FTP, Gopher, Telnet, NNTP, WAIS)를 받을 수 있다. 이때에 링크를 박스리스트에 등록해두면, 다음번 접속시에 신속히 참조할 수 있다. HTML+에 추가된 기능을 사용하면, 모자이크 이용자는 WWW문서를 가공할 수도 있다.

HTML이 HTML+언어로 하이퍼미디어를 작성

WWW는 하이퍼미디어 문서의 작성과 인식에 HTML을 사용한다.

HTML은 SGML과 같은 단순한 마크업(Markup)방식을 채용하고 있으며, 하이퍼 텍스트 문서를 서식화하는데 사용한다(WWW에는 통상 문서에 HTML이라는 접미어가 붙어있다). HTML로 단락, 항목, 번호항목, 원숫자 항목, 설명문 지정, 단락인용이라는 텍스트구성요소의 표시방식을 기술한다.

현재의 HTML사양은 하이퍼미디어 문서의 기본적인 작성과 레이아웃에 대응하는 것에 지나지 않으며, 그래서 기능이 매우 제한되어 있다.

확장판인 HTML+는 대형화 폼(Form), 이미지데이터 내의 하이퍼링크를 정의하는 핫스파트, 서식화된 표작성 등 보다 다양한 문서레이아웃 및 옵션, 스타일에 대응한다.

기존의 작성된 문서를 조사해 본다.

HTML문서는 보통의 텍스트형식이다. 표준 텍스트에디터(예,UNIX환경의 vi)를 사용하여 작성할 수 있는데, HTML은 기술하기 번거로운 언어이다.

그러나, 몇가지 Authoring Tool을 사용하면, 일반적인 텍스트로부터 자동적으로 HTML문서를 생성한다. HTML문서의 작성방법을 배우는데는 사람들이 어떻게 문서를 작성하는가를 조사하는 것도 한가지 방법이다. 대부분의 모자이크 브라우저에 구비된 소스버튼을 사용하여, 흥미있는 문서 및 페이지의 HTML코드를 볼 수 있고, 대부분의 HTML 문서는 충분히 이해할 수 있다. 이 HTML코드는 최종적인 그래픽 문서에 그대로 대응한다.

HTML코드를 사용하고 싶으면, 온라인 모자이크문서인 「A Beginner's Guide to HTML」을 천거한다. 이것은 WWW에서 이용할 수 있다.

결과를 보면서 편집할수 있다.

HTML문서는 WYSIWYG(What You See Is What You Get)기능을 가지는 에디터로 작성한다. 메뉴에 나타나는 Markup Tag를 선택해가는 방식의 에디터로도 만든다. HTML에디터에서, HTML로 쓰여진 문서로부터 가능한 화상을 대화적으로 표시할 수 있으므로 사용하기 쉽다. HTML을 사용한 에디터로는 Emacs의 현재 버젼이 있다.

이것은 「HTML MODE」를 준비하고 있는데,이용자가 HTML 코드를 기술하는 것을 지원한다. Windows용으로는 HTML Assistant라는 에디터가 있다. X-Window시스템 이용자용으로는 tkWWW가 HTML문을 WYSIWYG로 편집하는 기능을 가지고 있다. tkWWW는 브라우저에도 있는데, 작성한 문서를 즉시 표시해볼 수 있다. HotMetel은 X-

Window 시스템 및 Windows용 HTML+에디터이다. 매킨토시이용자는 BBEdit가 있는 HTML문서용 확장기능을 이용할수 있다.

〈 HTML Editor 와 Converter 〉

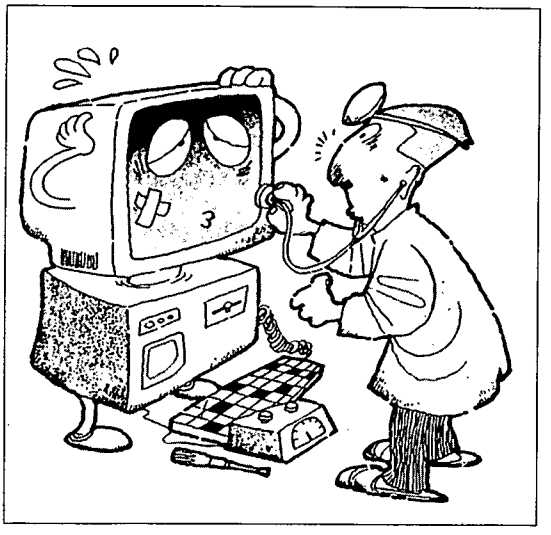
① BBEdit HTML : 매킨토시용 HTML 문서에디터
② Emacs Editor
③ HTML
④ HTML Assistant : MS Windows용 에디터로 HTML문서의 작성지원기능이 있음
⑤ HTML+
⑥ LaTex 2 HTML
⑦ Mail 2 HTML
⑧ RTF 2 HTML

하이퍼링크를 사용하여 WWW정보를 구축

WWW를 통하여 현재 억세스할 수 있는 정보에는 Telnet 및 Gopher, WAIS, FTP, Usenet news, Archie를 통하여 제공되는 정보와 Unix Manual Page 및 하이퍼미디어 문서형식의 정보가 있다. Mosaic는 인터넷에 축적된 기존의 정보자원을 연결시켜 구축된 광범위한 정보데이터베이스에 억세스할 수 있다. Mosaic를 사용하는 이용자는 효율적으로 WWW 내부를 항해할 수 있는 것이다.

URL로 억세스방법을 지정

URL(Uniform Resource Locator) WWW 문서에서 다른 화일의 위치를 표시하기 위해서 사용하는 형식으로, 현재 인터넷의 오브젝트 또는 정보자원을 특정짓는 규격안이



되고 있다. URL은 억세스하는 정보자원의 종별(예, Gopher 및 WAIS)와 화일의 Path를 표시하고 있다. 이용하는 서식은 「SCHEME명://HOST명.DOMAIN명(:PORT명)/PATH명/FILE명」으로 이루어진다. URL의 선두부분인 스킴명은 억세스방법의 종류를 지정한 것으로 다음과 같은 키워드를 지정할 수 있다.

▷ FTP : 로컬시스템이나 anonymous FTP 서버로부터 화일을 받는다.
▷ HTTP : WWW 서버로부터 화일을 받는다.(WWW에서 사용되는 Native Protocol).
▷ Gopher : Gopher서버에서 화일을 받는다
▷ WAIS : WAIS서버에서 화일을 받는다.
▷ News : 최신의 Usenet 뉴스를 읽는다.
▷ Telnet : 정보를 받을 때 Telnet Protocol로 접속한다.

「SCHEME명:」이하는 특정의 억세스수단을

나타낸다. 일반적으로 '//' 이하는 머신명 또는 옵션으로 포트번호를 표시한다. 나머지부분은 입수하고 자하는 화일명과 장소를 나타내는 PATH명을 기술한다. URL의 예를 보자.

▷ ftp://ftp.uu.net/info/README
▷ ftp://ftp.uu.net/usenet
▷ http://info.cern.ch:80/defaut.html
▷ news:alt.hypertext
▷ telnet://dra.com

프로토콜은 HTTP

HTTP(HyperText Transfer ProtocolZ)은 서버와 클라이언트간에 사용하는 프로토콜인데, HTTP를 사용할 때는 TCP/IP와 같은 신뢰성높은 전송서비스가 필요하다. 클라이언트는 서버와 Connection을 하고 요구명령을 보낸다. GET이라는 단어, 스페이스, 검색하고자하는 노드를 나타내는 URL의 일부, CR(Carriage Return), LF(Line Feed)로 구성된다.

이러한 요구명령에 대하여 서버는 요구된 노드에 있는 내용(Contents)을 HTML문서로 클라이언트에 보내고, 모든 콘텐트를 보내면 클라이언트와의 접속을 끊었다는 신호를 보낸다.

하이퍼링크로 문서를 연결한다.

WWW작성방법은 단순하다. WWW에서 사용할 문서에서 관련시키고 싶은 기존의 데이터로 하이퍼 링크를 설정하기만 하면 된다. 이 데이터를 공개하려면 FTP또는 HTTP DEMON을 실행할 필요가 있다. anonymous FTP가 이용할 수 있는 화일은, WWW로 링크를 설정할 필요가 있다. 이 방법은 서비스를 개시할 때의 노력이 적어도 되고, 매우 단기간에 공개하고 싶은 데이터를 인터넷을 경유하여 억세스가능하게 할 수 있다.

독자적으로 HTML을 기술하여 흥미를 끄는 데이터베이스에 링크를 확장하는 방법으로도, WWW를 작성할 수 있다. 데이터는 로컬로부터 가져와도, 또는 인터넷의 어디선가로부터 가져온다 고해도 좋다. 그러나, HTML언어에 익숙하여 인터넷에서 이용가능한 정보자원에 정통할 필요가 있다. 기존의 화일을 특별한 소프트웨어를 사용하면, 자동적으로 HTML문서로 변환할 수 있다.

공개할 것을 목적으로 문서를 작성할 때는 다음과 같은 가이드라인 따른다.

① 인터넷에서 정보에 억세스하는 대부분의 이용자는 정보를 열람하면서, 문서가 화면에 나타날 때까지 긴시간동안 기다리지 않으므로, 독자의 주의를 끌고 싶을 경우에만 그래픽을 사용해야 한다. 홈페이지에서 사용하는 이미지는 작아야 한다. 오브젝트가 무엇인가를 나타내는 단순한 아이콘으로 충분하다. 이용자가 아이콘을 선택하지도 않았는데 고품질의 이미지데이테를 문서내에 사용하는 것은 낭비이며, 네트워크의 부하를 늘리므로 주의하여야 한다.

② 네트워크를 경유하여 문서를 송신할때는, 로컬네트워크에 존재하는 문서를 표시하는 경우보다 속도가 늦어진다. 문서를 공개하기전에 타당성을 검증하는 의미에서 문서의 리모트억세스에 소요되는 시간을 검사해 보아야한다.

③ 이용자가 특정한 Hot-Word(특히 고해상도의 이미지데이터, 오디오 및 비디오용

디지털데이터를 사용하는 것)를 선택한 경우에는 몇바이트의 데이터가 전송되야 하는가를 보여주는 것이 좋다. 이용자는 이 수치를 보고 핫워드를 선택할 것인가 말것인가를 결정할 수 있다.

④ 서로 상이한 폰트 및 컬러 등이 하나의 화면에 존재하지 않도록하고, 양질의 그래픽 디자인원리를 적용한다. 교육목적으로 화면을 이용하거나, OHP화면에 투영하는 경우에는 이것은 특히 중요하다.

⑤ 「이것을 클릭하라」는 안내문을 사용하지 말고, 핫워드는 색 및 폰트를 변경하여 표시하는 것이 좋다.

⑥ 각 페이지 하단에는 문서에 관한 접촉선(전자메일 어드레스)을 표시해 주는 것이 좋다. 이것은 HTML어드레스태그를 사용하면 가능하다.

⑦ 한페이지를 넘지않는 것이 좋다.
계층화된 메뉴를 만들어서 의미있는 카테고리로 항목을 나누어 놓는 것이 좋다.

WWW, Gopher, WAIS를 비교한다

WWW, Gopher, WAIS는 모두 클라이언트/서버형식의 프리젠테이션 시스템이지만, 데이터모델이 다르다.

Gopher는 메뉴, 문서, 색인,에 의한 접속 등을 나타내는 데이터를 취급한다. WAIS는 취급하는 모든 데이터가 색인이다. 이 색인으로부터 모든 문서를 찾아낸다. 그에 비하여는 모두가 하이퍼텍스트문서이다. WWW는 Gopher와 WAIS데이터모델을 표현가능하다. 나아가 특별한 기능도 제공한다. WWW만 하이퍼링크를 가지고 있다. 텍스트는 세가지 시스템에서 모두 표시할 수 있지만, WWW는 보다 충실한 텍스트의 표시기능(예를 들면 표제, 리스트, 강조 등)를 표준으로 제공한다. 이미지, 오디오 및 비디오데이터는 모두 외부의 VIEW(예를 들면 MPEG Play라는 프로그램)에 대응한다. 이 세가지 시스템은 어플리케이션에 특화된 데이터를 취급하는 일이 적다. 데이터의 내부표현과 부호와에서도 다른 방법을 채용하고 있다. 또 세가지 시스템 모두 텍스트이외의 데이터를 제어하는 기능은 제한적이다.

원하는 정보를 찾기가 어렵다

현재의 분산형 하이퍼미디어시스템의 최대 제약은 어떤 정보가 변경되었는지, 어느 정보가 새로운 정보인지, 어떤 정보가 인터넷의 어디에 있는지를 간단하게 알 수 있는 방법이 없다는 것이다. Mosaic이용자는 모두 특정화제 및 테마에 관한 정보를 찾기 어렵다고 불평한다. 이용자가 인터넷에 관한 광범위한 지식을 가지고 있지 않아서, WWW에서 흥미있는 정보자원이 존재하는 장소를 찾아내기 어려운 경우도 많다. 다른 문제는 링크가 너무 많다는 것이다. 분산형 하이 퍼미디어 시스템 이용자는 억세스가능한 링크가 너무 많아서 압도되어 버린다.

모자이크는 이런 문제를 해결하는데 도움이 된다. 정보자원중에는 새롭게 만들어진 모자이크 서버의 정보를 화제로 제공하는 것도 있다. 예를 들면 아래의 두가지이다.

▷ WWW Virtual Library : 특정 테마에 관한 정보자원을 찾는데 최적의 장소이다.
▷ What's New With NCSA Mosaic : WWW의 새로운 서비스를 알려준다.

최근에는 검색용으로 색인을 자동 생성해주는

소프트웨어툴이 개발되고 있다. 예를 들자면,문서의내용을 색인으로 하는WebCrawker (http:/www. biotech. washington. edu/WebQuery. html)와 WWWWorm (http:/www/cs. colorado. edu/home/mcbryan/WWW.html)이 그것이다.

WWWWorm은 페이지타이틀과 URL내용에 기초하여 색인을 한다.

WWW 트래픽 증가가 현저하다

WWW의 지명도가 높아진다는 것은, NSFNet(National Science Foundation's North AmericanNetwork)의 네트워크 트래픽을 보아도 명백하다. 실제 인터넷백본 트래픽을 관찰하여 얻은 통계에 의하면, WWW의 트래픽은 최근 Gopher의 트래픽을 넘었다 (WWW브라우저는 Goper 서버에도 접속할 수 있으며, Gopher트래픽도 적지 않다).

CUSTOMIZE할 수 있도록 Mosaic를 확장한다.

많은 사람들이 모자이크용으로 인터페이스엔진을 구축중이다. 이용자가 WWW으로 이용가능한 다양한 타입의 인터넷데이터를 찾도록 지원한다.

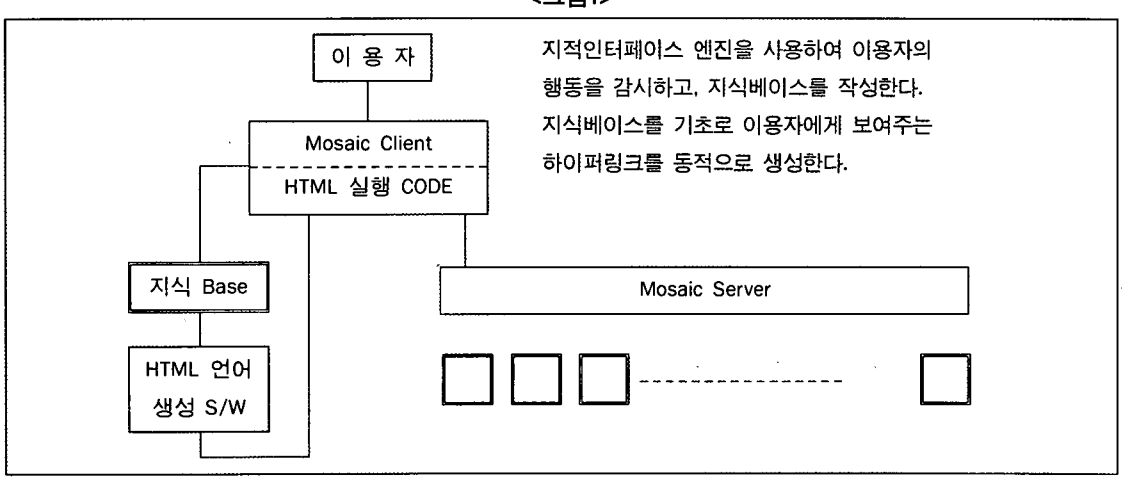
이러한 Approach는 자율적으로 Agent를 개발한 사람들이 채택한 것과 같은 것이다. 회의 Scheduling, 전자메일처리, 전자뉴스화일링, 오락기능선택 등에 대응하여 개개 이용자에게 맞도록 지원기능을 제공한다.

지식베이스에서 동적으로 링크를 만든다

지적 인터페이스 에이전트에서 모자이크을 강화한다는 것이다. 즉, 개개 이용자의 특별한 흥미, 습관, 기호를 학습하여 링크의 숫자를 조정하여 원하는 정보를 얻는데 도움을 주도록 한다. 이용자의 흥미와 기호에 대하여 배경이 되는 지식을 분야로하여 인터페이스 에이전트로 공급한다.

인터페이스 에이전트는 실행시에 이 지식을 이용하여, 이용자가 흥미를 가지는 정보를 볼 수 있게 해준다. 에이전트는 자율적으로 지식을 획득하지 않으면 안되는데, 이용자의 행동을 장시간 감시하여 지식베이스에 적절한 규칙

<그림1>



(Rule)과 사실(Fact)을 구축해 갈 필요가 있다(일종의 자기학습). 이 어프로치는 이용자의 고유한 흥미, 습관, 억세스패턴에 맞는 링크를 제공할 수 있도록, 모자이크를 Customize하는 것을 겨냥한다. 이 시스템은 룰 베이스알고리즘(Rule Base Algorithm), 뉴럴네트워크(Neural Network)를 사용하여 동적으로 링크를 만든다. 이렇게 모자이크가 가지고 있는 하이퍼미디어환경을 Customize한다. 이러한 접근은 현재의 고정된 하이퍼미디어시스템보다 유연하며, 특정한 화제에 대하여 매번 똑같은 링크를 정적으로 보여주는 것이 아니라, 보다 심오한 정보를 필요로하는 경우에는 그것에 맞는 기능을 제공한다. 이 그림1은 제안하는 시스템모델을 보여준다. 최초의 이용자(에이전트)는 특정한 흥미에 관한 정보를 지식베이스로 삼는다. 지식베이스룰과 팩트는 HTML언어생성 소프트웨어로 입력된다. 이용자고유의 HTML(링크)은 실행시에 생성된다. 특정화제 및 테마에 관련된 정보를 탐색하려면 다른 모자이크엔진 및 서버와 통신할 필요가 있다(Archie서버가 사용하는 방법도 유사하다).

디렉토리 서비스가 과제

WWW는 지금 급속하게 성장하고 있다. 인터넷의 분산형 하이퍼미디어시스템이 장래에도 활발하게 발전을 계속할 것은 명백하다. 하이퍼링크를 사용하는 설계는 유연하고, 기존의 WAIS와 Gopher라는 정보자원을 통합하는 것이다. 그래서 WWW는 장래의 연구 및 학문의 대상으로서 이상적이라고 생각된다.

또 고도의 대화적인 멀티미디어 어플리케이션은 보다 세련된 툴을 해결해야할 가장 중요한 문제는 프리젠테이션과 서비스의 품질면에서, WWW시스템 능력과 이용자요구에 미스매치(Miss-match)가 있다는 것. 적절한 디렉토리 서비스가 결여되어 있다는 것은 장래에 WWW 이용자를 더욱 번민하게 만든다는 것이다. 분산형 하이퍼미디어시스템에 관한 장래의 연구에서는, 이러한 문제에 어떻게 대처하느냐가 중요하다. *DC*

용어해설

- ▷ anonymous FTP : 누구나 자유롭게 화일을 받을 수 있는 FTP server.
- ▷ Archie : 공개된 FTP서버에 있는 화일을 색인등을 사용하여 검색할 수 있도록 한시스템.
- ▷ FTP : File Transfer Protocol. TCP/IP네트웍에서 사용하는 화일전송 프로토콜.
- ▷ GIF : Graphics Interchange Format. 컴퓨서브등에서 사용하는 화상데이커포맷.
- ▷ Gopher: 인터넷의 정보를 계층화하여 열람하기 위한 정보서비스.
- ▷ HTTP : Hyper Text Transfer Protocol. 하이퍼텍스트를 인터넷에서 교환하기 위해 WWW에서 사용하는 고유 프로토콜.
- ▷ SGML : Standard Generalized Markup Language. 문서논리 및 의미의 구조를 문서속에 간단한 마크를 부가하여 기술하는 언어. 국제표준규격.
- ▷ WWW : World Wide Web. 인터넷정보를 하이퍼텍스트형식으로 열람할 수 있도록 하는 시스템.

ABSTRACT

Database & Hackers
(The Emergence of the Cypherpunks)

The Cypherpunks first appeared in the fall of 1992. They made a public warning about the possible misuse of the escrow encryption system(commonly known as the Clipper Chip these days). Subsequent announcement of the Clipper Chip proposal by the Clinton administration in 1993 proved that the Cypherpunks are the powerful warriors on the frontline for the absolute total privacy of citizens. The public key cryptosystem, the first encryption system discovered in the private sector, is very resistant to all known cryptanalysis, and is suitable for use in the internet environment. So the Cypherpunks want the society where everyone can get total privacy by using public key cryptosystem. In fact, total privacy for everyone-including tax evaders, criminals, and terrorists-will change the current society in an unrepairable way. For example, untraceable digital cash will diminish the power of the existing nations to the nill. Or the traceable digital cash might lead to a totalitarian society. There must be a compromise somewhere between the protection by the public law and the protection by oneself. The Cypherpunks think that the disappearance of the existing nations is quite natural in the process of the human history. They also think the future society will be characterized as the capitalistic anarchy. The choice is in our hands, now.