(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 15/00

(11) 공개번호 특1997-0012183
(43) 공개일자 1997년03월29일

(21) 출원번호 특1996-0034970
(22) 출원일자 1996년08월19일
(30) 우선권주장 8/516,671 1995년08월18일 미국(US)
(71) 출원인 썬 마이크로시스템스 인코포레이티드 리 페치
미합중국, 캘리포니아 94043 마운틴 뷰, 가르시아 애비뉴 2550
(72) 발명자 네셋 데니 엠.
미합중국 캘리포니아 94555, 프레몬트, 와바시 리버 플레이스 34810
터크테런디
미합중국 캘리포니아 94086, 써니베일, 어베일러 드라이브 #100 1260
(74) 대리인 원석희, 박해천

심사청구 : 없음

(54) 분산 시스템에서의 자원 억세스를 안전하게 제어하기 위한 방법 및 시스템

요약

1. 청구범위에 기재된 발명이 속하는 기술분야

컴퓨터 시스템에서의 안전성을 제공하면서 구룹 식별을 이용한 시스템 지원의 억세스.

2. 발명이 해결하고자 하는 기술적과제

네트워크 환경내 분산 컴퓨터 시스템에서, 다양한 서버로부터의 억세스 요청을 안전하게 다루는 문제를 정밀하고 간단한 방법으로 해결한다.

3. 발명의 해결방법의 요지

본 발명의 실시예는 분산 컴퓨터 시스템에서 자원 억세스를 안전하게 제어하기 위한 방법 및 시스템을 제공한다. 본 발명의 일 실시예는 타겟 객체에 구룹 식별을 저장하고 설정하여 타겟 객체 억세스를 요청하는 클라이언트 객체가 이 구룹의 회원인가를 결정하는 회원제 검사를 사용한다. 이러한 방법에 있어서 본 발명은 객체 요청의 억세스 권리를 검증하기 위하여 일부 종래 기술의 시스템에서 일반적인 값비싼 암호화 오퍼레이션 수행을 사용하지 않는다.

본 발명의 제2실시예는 타겟 객체 참조에 구룹 식별을 저장하고 설정하여 시스템내의 클라이언트 객체에 타겟 객체 참조를 전단한다. 타겟 객체 참조는 구룹 식별 엔트리를 포함하고 있기 때문에, 제1클라이언트 객체는 시스템내의 다른 클라이언트들이 식별된 구룹의 회원인가를 결정할 수 있다. 이러한 결정은, 타겟 객체를 위한 서버와 우선적으로 통신하지 않고, 제1클라이언트 객체가 타겟 객체 참조를 구룹의 다른 회원들에게 전달하도록 허용한다. 이러한 방법에 있어서, 본 발명은 타겟 객체를 위한 서버와의 통신에 따른 값비싼 트랜잭션 비용을 피할 수 있다.

4. 발명의 중요한 용도

서버 및 클라이언트를 사용하는 컴퓨터 관련 시스템.

대표도

도2

명세서

[발명의 명칭]

분산 시스템에서의 자원 억세스를 안전하게 제어하기 위한 방법 및 시스템

[도면의 간단한 설명]

제1도는 본 발명의 바람직한 실시예를 구현하기 위한 컴퓨터 시스템의 블록도,

제2도는 시스템 억세스를 안전하게 제어하기 위한 제1실시예의 바람직한 단계를 설명하는 흐름도.

본 내용은 요부공개 건이므로 전문 내용을 수록하지 않았음.

(57) 청구의 범위

청구항 1

스프레드쉬트 객체에 그룹 식별자를 묶기 위한 요청을 클라이언트 객체에서 스프레드쉬트 서버로 보내는 단계; 상기 스프레드쉬트 서버의 제어하에서, 스프레드쉬트 객체를 얻는 단계; 상기 스프레드쉬트 객체에 구룹 식별자를 저장하는 단계; 위조 불가능 검사합계를 발생하는 단계; 스프레드쉬트 객체에 위조 불가능 검사합계를 저장하는 단계; 위조 불가능 검사합계를 클라이언트 객체로 보내는 단계; 상기 클라이언트 객체의 제어하에서, 복합 다큐먼트를 인쇄하기 위하여 요청을 복합 다큐먼트 서버로 보내는 단계; 상기 복합 다큐먼트 서버의 제어하에서, 상기 스프레드쉬트가 서버 스프레드쉬트 객체로부터의 데이타를 다시 보낼것을 요구하면서 구룹 식별자 및 위조 불가능 검사합계를 포함하는 요청을 상기 스프레그쉬트 서버에 보내는 단계; 상기 스프레드쉬트 서버의 제어하에서, 구룹 식별자의 분석에 기초한 스프레드쉬트 객체의 억세스를 허용하거나 거잘하는 단계를 포함하여 이루어지는 것을 특징으로 하는 분산 컴퓨터 시스템에서 시스템 지원의 억세스를 제어하기 위하여 컴퓨터 시스템에서 수행되는 방법.

청구항 2

클라이언트 객체, 제1서버 객체, 타겟 객체 및 제2서버 객체를 포함하고, 각각의 객체는 컴퓨터 시스템내에 탑제된 하나 이상의 특정 구룹에 속하는 분산 컴퓨터 시스템에서 시스템 지원의 억세스를 제어를 용이하게 하기 위하여 상기 컴퓨터 시스템에서 수행되는 방법에 있어서, 상기 제1서버 객체의 제어하에서, 상기 시스템내의 구룹이 상기 타겟 객체의 억세스 특권인지를 식별하도록 상기 타겟 객체에 구룹식별자를 저장하는 단계; 상기 제2서버 객체의 제어하에서, 컨테이너 객체를 얻는 단계; 상기 타겟 객체의 억세스르 요구하면서, 상기 제2서버 객체가 동작하게 되는 사용자를 식별하는 사용자 식별자를 포함하는 요청을 제1서버 객체에 보내는 단계; 상기 제1서버의 제어하에서, 상기 타겟 객체에 저장된 상기 구룹 식별자 및 상기 제2서버로부터의 요청에 포함되어 있는 사용자 식별자를 사용하여 상기 제2서버가 상기 타겟 객체를 억세스하도록 허락받았는지를 검증하는 단계를 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 3

제2항에 있어서, 상기 컨테이너 객체를 얻는 단계는, 상기 제1서버 객체의 제어하에서, 상기 컴퓨터 시스템내의 상기 타겟 객체의 위치를 나타내는 타겟 객체 참조를 클라이언트 객체로 보내는 단계; 상기 클라이언트 객체의 제어하에서, 상기 클라이언트 객체가 속하는 구룹의 회원을 위하여 동작하는 제2서버를 위치시키는 단계; 상기 제2서버가 상기 타겟 객체를 참조하는 컨테이터 객체를 얻을 것을 요청하면서, 상기 클라이언트 객체가 속하는 상기 구룹을 식별하는구룹식별자를 포함하고 상기 클라이언트 객체로부터 상기 타겟 객체 참조를 포함하는 성기 제2서버 객체로 요청을 상기 위치된 제2서버로 보내는 단계; 상기 제2서버의 제어하에서, 상기 컨테이너 객체를 얻는 단계; 및 상기 컨테이너 객체내에 상기 타겟 객체 참조 및 상기 구룹 식별자를 저장하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 4

제2항에 있어서, 상기 제2서버에서 상기 제1서버로 상기 요청을 보내는 단계는, 상기 클라이언트 객체의 제어하에서, 상기 컨테이너 객체를 사용하기 위하여 상기 컨테이너 객체를 위한 상기 참조 및 클라이언트 객체의 사용자를 위한 식별자를 포함하는 요청을 제2서버로 보내는 단계; 상기 제2서버의 제어하에서, 상기 클라이언트로부터의 요청에 응답하여, 상기 타겟 객체의 억세스화도록, 상기 제2서버 객체가 동작하게 되는 사용자를 위한 식별자 및 상기 타겟 객체를 위한 상기 참조를 포함하는 요청을 상기 제1서버로 보내는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 5

제4항에 있어서, 상기 제1서버의 제어하에서, 상기 제2서버로부터 상기 제1서버로 보내어진 사용자의 식별을 사용하여 제2서버를 인증하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 6

제5항에 있어서, 상기 제2서버가 인증되어 상기 타겟 객체를 억세스할 권리를 갖는 상기 구룹의 회원임이 결정되었을 때, 상기 제1서버를 위한 참조로부터 위조불가능 회원을 검색하고, 검색된 위조 불가능 회원을 상기 타겟 객체에 저장된 위조 불가능 회원과 비교함으로써, 제2서버가 요청된 방법에서 상기 타겟 객체를 억세스 하도록 인증받았는지를 결정하는 단계; 및 상기 위조 불가능 회원들이 일치하면, 상기 제2서버의 억세스 권리에 의해 상기 제2서버가 상기 타겟 객체를 억세스 하도록 허락하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 7

제2항에 있어서, 상기 제2서버가 상기 타겟 객체를 억세스하기 위한 허락을 가지는지를 검증하는 단계는, 상기 제1서버의 제어하에서, 상기 타겟 객체로부터의 상기 구룹 식별자를 검색하는 단계; 상기 주사용작 상기 타겟 객체의 억세스 권리를 갖는 구룹 회원인가를 결정하기 위한 요청과 함께 상기 검색된 구룹 식별자 및 상기 사용자 식별자를 회원제 메카니즘으로 보내는 단계; 및 상기 타겟 객체의 억세스 권리를 갖는 구룹의 회원인 사용자를 위하여 상기 제2서버가 동작하는 것으로 결정되면, 상기 제2서버가 상기 타겟 객체를 억세스하도록 허락하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 8

제2항에 있어서, 상기 제1서버 객체가 상기 타겟 객체를 생성하여야 하는지를 지시하는 요청을 상기 클

라이언트 객체로부터 상기 제1서버 객체로 보내는 단계; 및 상기 제1서버 객체의 제어하에서, 타겟 객체를 생성하는 단계; 및 상기 타겟 객체에 관하여 구룹 회원이 가지는 억세스 권리의 지시를 저장하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 방법.

청구항 9

클라이언트 객체, 제1서버 객체, 타겟 객체 및 제2서버 객체를 포함하고, 각각의 객체는 컴퓨터 시스템 네내에 탑제된 하나 이상의 특정 구룹에 속하는 분산 컴퓨터 시스템에서 시스탬 지원의 억세스를 제어를 용이하게 하기 위한 컴퓨터 시스템에 있어서, 상기 제1서버 객체가, 상기 시스템내의 구룹이 상기 타겟 객체의 억세스 특권인지를 식별하도록 상기 타겟 객체에 구룹식별자를 저장하도록 구성되고; 상기 제2서버 객체가, 컨테이너 객체를 얻고, 상기 타겟 객체의 억세스를 요구하면서, 상기 제2서버 객체가 동작하게 되는 사용자를 식별하는 사용자 식별자를 포함하는 요청을 제1서버 객체에 보내도록 구성되며; 상기 제1서버가, 상기 타겟 객체에 저장된 상기 구룹 식별자 및 상기 제2서버로부터의 요청에 포함되어 있는 사용자 식별자를 사용하여 상기 제2서버가 상기 타겟 객체를 억세스할 허락을 가지고 있는지를 검증하도록 구성되는 시스템을 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 시스템.

청구항 10

제9항에 있어서, 상기 컨테이너 객체를 얻는 것은, 상기 제1서버 객체가, 상기 컴퓨터 시스템내의 상기 타겟 객체의 위치를 나타내는 타겟 객체 참조를 클라이언트 객체로 보내도록 구성되고; 상기 클라이언트 객체가 상기 클라이언트 객체가 속하는 구룹의 회원을 위하여 동작하는 제2서버를 위치시키고, 상기 제2서버가 상기 타겟 객체를 참조하는 컨테이터 객체를 얻을 것을 요청하면서, 상기 클라이언트 객체가 속하는 상기 구룹을 식별하는 구룹식별자를 포함하고 상기 클라이언트 객체로부터 상기 타겟 객체 참조를 포함하는 성기 제2서버 객체로의 요청을 상기 위치된 제2서버로 보내도록 구성되고; 상기 제2서버가, 상기 컨테이너 객체를 얻고, 상기 컨테이너 객체내에 상기 타겟 객체 참조 및 상기 구룹 식별자를 저장하도록 구성되는 시스템을 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 시스템.

청구항 11

제9항에 있어서, 상기 제2서버에서 상기 제1서버로 상기 요청을 보내는 것은, 상기 클라이언트 객체가, 상기 컨테니너 객체를 사용하기 위하여 상기 컨테이너 객체를 위한 상기 참조 및 클라이언트 객체의 사용자를 위한 식별자를 포함하는 요청을 제2서버로 보내도록 구성되고; 상기 제2서버가, 상기 클라이언트로부터의 상기 요청에 응답하여, 상기 타겟 객체의 억세스하도록, 상기 제2서버 객체가 동작하게 되는 사용자를 위한 식별자 및 상기 타겟 객체를 위한 상기 참조를 포함하는 요청을 상기 제1서버로 보내도록 구성되는 시스템을 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 시스템.

청구항 12

제11항에 있어서, 상기 제1서버가, 상기 제2서버로부터 상기 제1서버로 보내어진 사용자의 식별을 사용하여 제2서버를 인증하도록 구성되는 시스템을 더 포함하여 이루어지는 것을 특징으로 하는 장치.

청구항 13

제12항에 있어서, 상기 제2서보가 인증되어 상기 타겟 객체를 억세스할 권리를 갖는 상기 구룹의 회원임이 결정되었을 때, 상기 제1서버를 위한 참조로부터 위조불가능 회원을 검색하고, 검색된 위조 불가능 회원을 상기 타겟 객체에 저장된 위주 불가능 회원과 비교함으로써, 제2서버가 요청된 방법에서 상기 타겟 객체를 억세스하도록 인증받았는지를 결정하도록 구성되고; 상기 위조 불가능 회원들이 일치하면, 상기 제2서버의 억세스 권리에 의해 상기 제2서버가 상기 타겟 객체의 억세스를 허락하도록 구성된 메카니즘을 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 시스템.

청구항 14

제9항에 있어서, 상기 제2서버가 상기 타겟 객체를 억세스할 허락을 가지고 있는지를 검증하는 것은, 상기 제1서버가, 상기 타겟 객체로부터의 상기 구룹 식별자를 검색하고; 상기 주사용작 상기 타겟 객체의 억세스 권리를 갖는 구룹 회원인가를 결정하기 위한 요청과 함께 상기 검색된 구룹 식별자 및 상기 사용자 식별자를 회원제 메카니즘으로 보내도록 구성되고, 상기 타겟 객체의 억세스 권리를 갖는 구룹의 회원인 사용자를 위하여 상기 제2서버가 동작하는 것으로 결정되면, 상기 제2서버가 상기 타겟 객체의 억세스를 허락하도록 구성된 시스템을 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 시스템.

청구항 15

제9항에 있어서, 상기 제1서버 객체가 상기 타겟 객체를 생성하여야 하는지를 지시하는 요청을 상기 클라이언트 객체로부터 상기 제1서버 객체로 보내도록 구성된 메카니즘을 더 포함하고, 상기 제1서버 객체는, 타겟 객체를 생성하고; 상기 타겟 객체에 관하여 구룹 회원이 가지는 억세스 권리의 지시를 저장하도록 구성되는 것을 특징으로 하는 컴퓨터 시스템.

청구항 16

클라이언트 객체, 제1서버 객체, 타겟 객체 및 제2서버 객체를 포함하고, 각각의 객체는 컴퓨터 시스템 네내에 탑제된 하나 이상의 특정 구룹에 속하는 분산 컴퓨터 시스템에서 시스템 지원의 억세스를 제어를 용이하게 하기 위한 컴퓨터 프로그램에 있어서, 상기 시스템내의 구룹이 상기 타겟 객체의 억세스 특권인지를 식별하도록 상기 타겟 객체에 구룹 식별자를 저장하도록 구성된 상기 제1서버 객체를 위한 코드; 컨테이너 객체를 얻고, 상기 타겟 객체의 억세스를 요구하면서, 상기 제2서버 객체가 동작하게 되는 사용자를 식별하는 사용자 식별자를 포함하는 요청을 제1서버 객체에 보내도록 구성된 상기 제2서버 객체를 위한 코드; 상기 타겟 객체에 저장된 상기 구룹 식별자 및 상기 제2서버로부터의 요청에 포함되어 있

는 사용자 식별자를 사용하여 상기 제2서버가 상기 타겟 객체를 억세스할 허락을 가지고 있는지를 검증하도록 구성된 상기 제1서버를 위한 코드를 포함하며, 상기 코드들은 유형매체에 저장되는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 17

제16항에 있어서, 상기 컨테이너 객체를 얻는 것은, 상기 컴퓨터 시스템내의 상기 타겟 객체의 위치를 나타내는 타겟 객체 참조를 클라이언트 객체로 보내도록 구성된 상기 제1서버 객체를 위한 코드; 상기 클라이언트 객체가 속하는 구룹의 회원을 위하여 동작하는 제2서버를 위치시키고, 상기 제2서버가 상기 타겟 객체를 참조하는 컨테이터 객체를 얻을 것을 요청하면서, 상기 클라이언트 객체가 속하는 상기 구룹을 식별하는 구룹 식별자를 포함하고 상기 플라이언트 객체로부터 상기 타겟 객체 참조를 포함하는 성기 제2서버 객체로의 요청을 상기 위치된 제2서버로 보내도록 구성된 상기 클라이언트 객체를 위한 코드; 상기 컨테이너 객체를 얻고, 상기 컨테이너 객체내에 상기 타겟 객체 참조 및 상기 구룹 식별자를 저장하도록 구성된 상기 제2서버를 위한 코드를 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 18

제16항에 있어서, 상기 제2서버에서 상기 제1서버로 상기 요청을 보내는 것은, 상기 컨테이너 객체를 사용하기 위하여 상기 컨테이너 객체를 위한 상기 참조 및 클라이언트 객체의 사용자를 위한 식별자를 포함하는 요청을 제2서버로 보내도록 구성된 상기 클라이언트 객체를 위한 코드 상기 클라이언트로 부터의 상기 요청에 응답하여, 상기 타겟 객체의 억세스하도록, 상기 제2서버 객체가 동작하게 되는 사용자를 위한 식별자 및 상기 타겟 객체를 위한 상기 참조를 포함하는 요청을 상기 제1서버로 보내도록 구성된 상기 제2서버를 위한 코드를 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 19

제18항에 있어서, 상기 제2서버로부터 상기 제1서버로 보내어진 사용자의 식별을 사용하여 제2서버를 인증하도록 구성된 상기 제1서버를 위한 코드를 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 20

제12항에 있어서, 상기 제2서버가 인증되어 상기 타겟 객체를 억세스할 권리를 갖는 상기 구룹의 회원임이 결정되었을 때, 상기 제1서버를 위한 참조로부터 위조 불가능 회원을 검색하고, 검색된 위조 불가능 회원을 상기 타겟 객체에 저장된 위조 불가능 회원과 비교함으로써, 제2서버가 요청된 방법에서 상기 타겟 객체를 억세스 하도록 인증받았는지를 결정하고; 상기 위조 불가능 회원들이 일치하면, 상기 제2서버의 억세스 권리에 의해 상기 제2서버가 상기 타겟 객체의 억세스를 허락하는 코드를 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 21

제16항에 있어서, 상기 제2서버가 상기 타겟 객체를 억세스할 허락을 가지고 있는 지를 검증하는 것은, 상기 타켓 객체로부터의 상기 구룹 식별자를 검색하고; 상기 주사용작 상기 타겟 객체의 억세스 권리를 갖는 구룹회원인가를 결정하기 위한 요청과 함께 상기 검색된 구룹 식별자 및 상기 사용자 식별자를 회원제 메카니즘으로 보내고; 상기 타겟 객체의 억세스 원리를 갖는 구룹의 회원인 사용자를 위하여 상기 제2서버가 동작하는 것으로 결정되면, 상기 2서버가 상기 타겟 객체의 억세스를 허락하도록 구성된 상기 제1서버를 위한 코드를 더 포함하여 이루어지는 것을 특징으로 하는 컴퓨터 프로그램.

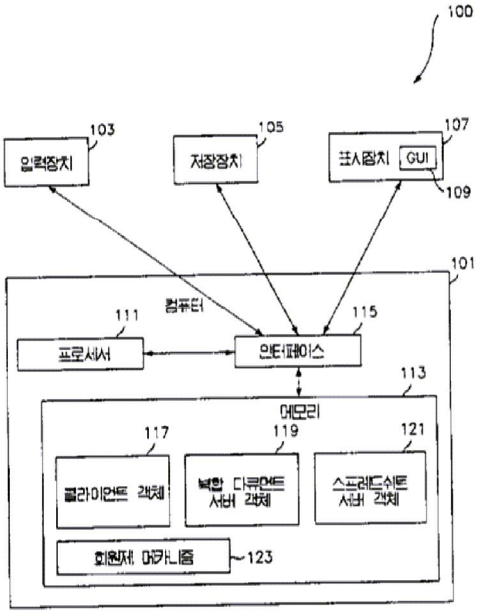
청구항 22

제16항에 있어서, 상기 제1서버 객체가 상기 타겟 객체를 생성하여야 하는지를 지시하는 요청을 상기 클라이언트 객체로부터 상기 제1서버 객체로 보내도록 구성된 코드를 더 포함하고, 상기 제1서버 객체를 위한 코드는, 타겟 객체를 형성하고; 상기 타겟 객체에 관하여 구룹 회원이 가지는 억세스 권리의 지시를 저장하도록 구성되는 것을 특징으로 하는 컴퓨터 프로그램.

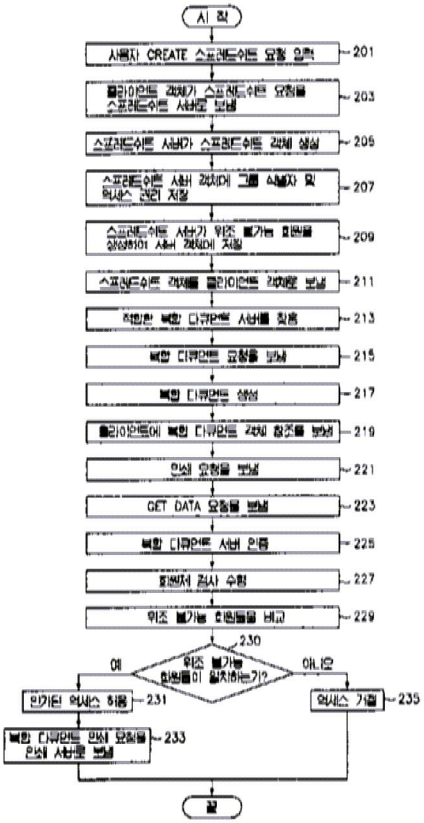
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

도면1


100
103
입력장치
105
저장장치
107
표시장치
GUI
109
101
컴퓨터
111
프로세서
115
인터페이스
113
메모리
117
119
121
클라이언트 객체
복합 다큐먼트 서버 객체
스크랩북 서버 객체
회원제 메카니즘
123

도면2


시작
사용자 CREATE 스크랩북 요청 입력
201
클라이언트 객체가 스크랩북 요청을 스크랩북 서버로 보냄
203
스크랩북 서버가 스크랩북 객체 생성
205
스크랩북 서버 객체에 그룹 식별자 및 억세스 관리 저장
207
209
211
213
215
217
219
221
GET DATA 요청을 보냄
223
225
227
229
230
예
아니오
인가된 억세스 허용
231
억세스 거절
235
233
끝