(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년05월04일
(11) 등록번호 10-1516708
(24) 등록일자 2015년04월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *H04L 9/32* (2006.01)
H04N 7/18 (2006.01)
(21) 출원번호 10-2011-7024357
(22) 출원일자(국제) 2010년03월25일
심사청구일자 2014년08월22일
(85) 번역문제출일자 2011년10월17일
(65) 공개번호 10-2012-0028298
(43) 공개일자 2012년03월22일
(86) 국제출원번호 PCT/JP2010/002119
(87) 국제공개번호 WO 2010/116642
국제공개일자 2010년10월14일
(30) 우선권주장
JP-P-2009-081307 2009년03월30일 일본(JP)
(56) 선행기술조사문헌
JP2006086936 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세콤 가부시키가이샤
일본국 도쿄도 시부야쿠 진구마에 1쵸메 5반 1고
(72) 발명자
후지사와 마사유키
일본국 181-0013 토쿄도 미타카시 시모렌자쿠 6쵸메 11-23 세콤 가부시키가이샤 내
(74) 대리인
송봉식, 정삼영

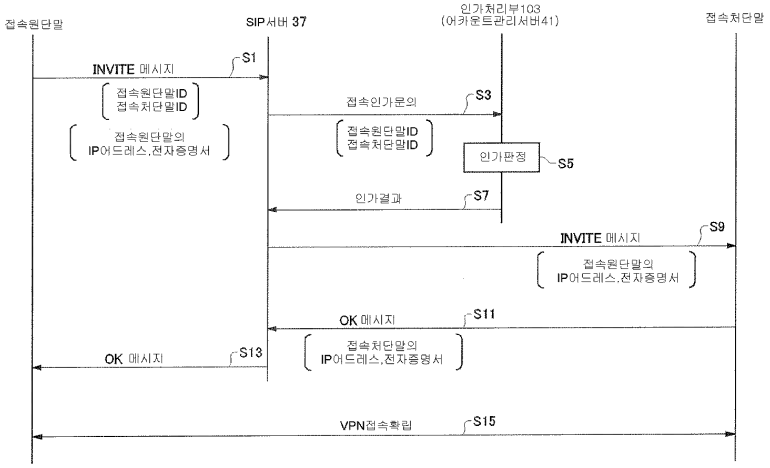
전체 청구항 수 : 총 4 항 심사관 : 문남두

(54) 발명의 명칭 **감시 시스템 및 통신 관리 장치**

(57) 요 약

통신 관리 장치(11)는 복수의 단말과 접속된다. 복수의 단말은 감시 장치(15) 및 이용자 장치(17)이다. 단말간의 통신을 행할 때, 접속원의 단말이 SIP의 초대 메시지를 통신 관리 장치(11)에 송신한다. 통신 관리 장치(11)에는, SIP 서버(37)에 더하여, 접속이 인가될 단말의 조합을 기억한 접속 인가 정보를 기억한 인가 정보 기억부 (101)와, 접속 인가 정보를 참조하여 단말 간의 접속을 인가하는 인가 처리부 (103)가 구비된다. SIP 서버(37)가 접속원의 단말로부터 초대 메시지를 취득했을 때, 인가 처리부 (103)가 접속원 및 접속처의 단말의 접속을 인가한 경우에, SIP 서버(37)가 접속원의 단말로부터의 초대 메시지를 접속처의 단말에 공급한다. 이것에 의해, 감시 시스템에 SIP를 적용하는 경우의 세큐러티를 향상할 수 있는 감시 시스템이 제공된다.

대 표 도



명 세 서

청구범위

청구항 1

감시대상에 설치된 감시대상측의 단말과, 상기 감시대상측의 단말로부터 수신한 감시 정보를 이용하는 이용자측에 설치된 이용자측의 단말과, 상기 감시대상측의 단말과 상기 이용자측의 단말과의 통신을 관리하는 통신 관리 장치를 가진 감시 시스템으로서,

상기 감시대상측의 단말 또는 상기 이용자측의 단말의 일방이 타방에 접속을 요구할 때, 이 접속원의 단말은 접속처의 단말의 식별 정보를 포함하는 SIP의 초대 메시지를 상기 통신 관리 장치에 송신하도록 구성되고,

상기 통신 관리 장치는,

SIP 서버와,

접속이 인가될 감시대상측의 단말과 이용자측의 단말을 대응시킨 조합을 나타내는 접속 인가 정보를 기억한 인가 정보 기억부와,

상기 접속 인가 정보를 참조하여 감시대상측의 단말과 이용자측의 단말과의 접속을 인가할지 아닐지를 판정하는 인가 처리부를 갖고,

상기 SIP 서버는,

상기 접속원의 단말로부터 상기 초대 메시지를 취득했을 때, 상기 초대 메시지에 포함되는 상기 접속처의 단말의 식별 정보를 상기 인가 처리부에 공급하고, 상기 인가 처리부가 감시대상측의 단말과 이용자측의 단말과의 접속을 인가한 경우에, 상기 SIP 서버가 상기 접속원의 단말로부터의 초대 메시지를 상기 접속처의 단말에 공급하고,

상기 접속처의 단말은 상기 초대 메시지를 상기 통신 관리 장치로부터 수신했을 때에 SIP의 OK 메시지를 상기 통신 관리 장치에 송신하고,

상기 초대 메시지 및 상기 OK 메시지에는, SIP 세션 확립 후에 상기 접속원 및 접속처의 단말 간에 상기 통신 관리 장치를 통하지 않는 단말 간 접속을 확립하기 위하여 사용되는 접속 확립 정보가 부가되고,

상기 초대 메시지는 상기 접속원의 단말의 IP 어드레스와 전자증명서를 상기 접속 확립 정보로서 포함하고, 상기 OK 메시지는 상기 접속처의 단말의 IP 어드레스와 전자증명서를 상기 접속 확립 정보로서 포함하는 것을 특징으로 하는 감시 시스템.

청구항 2

제 1 항에 있어서, 상기 통신 관리 장치를 통하지 않는 단말 간 접속은 단말 간에 VPN을 구축하여 접속하는 단말 간 VPN인 것을 특징으로 하는 감시 시스템.

청구항 3

삭제

청구항 4

제 1 항 또는 제 2 항에 있어서, 상기 통신 관리 장치와 상기 복수의 단말과의 접속은 상기 통신 관리 장치와 상기 복수의 단말 사이에 VPN을 구축한 센터 단말 간 VPN에 의해 접속되어 있고,

상기 SIP 서버는 상기 센터 단말 간 VPN을 통하여 상기 복수의 단말과 SIP 메시지를 통신하는 것을 특징으로 하는 감시 시스템.

청구항 5

제 1 항 또는 제 2 항에 있어서, 상기 감시 정보는 상기 감시대상에서 촬영된 화상, 상기 감시대상에서 검출된

감시 신호, 상기 이용자측에서 생성된 제어 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 감시 시스템.

청구항 6

삭제

청구항 7

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 감시 정보를 취득하는 감시대상의 단말과, 감시 정보를 입수하여 이용하는 이용자측의 단말을 통신 가능하게 접속한 감시 시스템에 관한 것이다.

배 경 기 술

[0002] 종래, 점포, 공장 등의 감시대상에 감시 카메라를 설치하고, 감시 영상을 원격지에서 감시하는 감시 시스템이 실용화되어 있다. 감시 영상은 원격의 감시 센터에 송신되고, 또한 감시대상의 소유자(오너)의 사무소에 송신된다. 감시 영상의 송신에는 ISDN 등의 일반 공중회선이 사용된다(예를 들면, 특허문헌 1).

[0003] 최근, ADSL이나 FTTH와 같은 브로드밴드 회선의 보급에 의해, 감시 시스템에 있어서의 감시 영상 등의 송수신을 인터넷상에서 실현하는 것에 대한 요구가 향상되고 있다. 인터넷의 이용에 의해, 비용의 절감이나, 시스템의 유연성의 향상을 기대할 수 있다.

[0004] 인터넷상에서 음성이나 영상을 전송하는 기술로서는 SIP(Session Initiation Protocol)라고 불리는 프로토콜이 알려져 있다. SIP는 IP 전화나 텔레비전 회의 등에 적용된다. SIP에서 2거점 사이를 접속하기 위해서는, SIP 서버에 각 거점의 어드레스가 등록된다. 이것에 의해, 어드레스가 등록된 거점 간에 SIP의 통신이 가능하게 된다.

[0005] 그러나, 감시 시스템에 SIP를 적용하려고 하면, 세큐러티상의 문제를 생각할 수 있다. 즉, 감시대상의 영상 등을 외부로부터 감시하는 감시 시스템에서는 높은 세큐러티성이 요구된다. 이것에 대하여, SIP에서는, 어드레스를 등록함으로써 임의의 거점 사이를 접속할 수 있다. 그 때문에 감시 시스템에 SIP를 그대로 적용하는 것은 세큐러티성의 관점에서 바람직하지 않다.

[0006] 예를 들면, 감시대상이 점포이며, 복수의 점포의 단말이 감시 센터에 접속되었다고 가정한다. 감시 센터는 각 점포의 오너의 단말과도 접속된다. 이 경우, 각 점포의 단말에 접속할 수 있는 것은 해당하는 오너의 단말에 한정되어야 한다.

[0007] 그러나, 종래의 SIP에서는, SIP 서버에 어드레스가 등록되어 있는 임의의 단말 사이에 접속이 가능하다. SIP 서버는 기본적인 인증 기능으로서 패스워드 및 ID의 인증은 행하는 것이 가능하다. 그러나, 이것은, 단말과 SIP 서버 사이의 인증에 한정된다. 단말과 SIP 서버의 접속이 허가되어 버리면, SIP 서버를 통한 단말끼리의 조합을 제한할 수는 없다. 따라서, 점포의 단말과 오너 단말 사이의 접속을 제한할 수도 없다. 그 때문에 오너가 자신 이외의 점포의 감시 정보를 입수할 수 있을 가능성이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 일본 특개 2001-54102호 공보

발명의 내용

해결하려는 과제

[0009] (발명의 개요)

[0010] (발명이 해결하고자 하는 과제)

[0011] 본 발명은 상기 배경하에 이루어진 것이다. 본 발명의 목적은 감시 시스템에 SIP를 적용하는 경우의 세큐러티를 향상할 수 있는 감시 시스템을 제공하는 것에 있다.

과제의 해결 수단

[0012] 본 발명의 1의 태양은 감시 시스템이며, 이 감시 시스템은 감시 정보를 통신하는 복수의 단말과, 복수의 단말의 통신을 관리하는 통신 관리 장치를 갖고, 복수의 단말의 각각이 감시대상측 또는 감시대상으로부터 수신한 감시 정보를 이용하는 이용자측에 설치된 감시 시스템으로서, 복수의 단말 중 하나가 다른 단말에 접속을 요구할 때, 이 접속원의 단말은 접속처의 단말의 식별 정보를 포함하는 SIP의 초대 메시지를 통신 관리 장치에 송신하도록 구성되고, 통신 관리 장치는 SIP 서버와, 접속이 인가될 단말의 조합을 나타내는 접속 인가 정보를 기억한 인가 정보 기억부와, 접속 인가 정보를 참조하여 단말 간의 접속을 인가할지 아닐지를 판정하는 인가 처리부를 갖고, SIP 서버는, 접속원의 단말로부터 초대 메시지를 취득했을 때, 초대 메시지에 포함되는 접속처의 단말의 식별 정보를 인가 처리부에 공급하고, 인가 처리부가 단말 간의 접속을 인가한 경우에, SIP 서버가 접속원의 단말로부터의 초대 메시지를 접속처의 단말에 공급한다.

[0013] 본 발명의 다른 태양은 통신 관리 장치이며, 이 통신 관리 장치는 감시 정보를 통신하는 복수의 단말의 통신을 관리하는 통신 관리 장치로서 SIP 서버와, 접속이 인가될 단말의 조합을 나타내는 접속 인가 정보를 기억한 인가 정보 기억부와, 접속 인가 정보를 참조하여 단말 간의 접속을 인가할지 아닐지를 판정하는 인가 처리부 갖고, SIP 서버가, 복수의 단말 중 하나로부터, 다른 단말로의 식별 정보를 포함하는 SIP의 초대 메시지를 취득했을 때, 인가 처리부 초대 메시지에 포함되는 접속처의 단말의 식별 정보에 근거하여, 단말 간의 접속을 인가할지 아닐지를 판정하고, 인가 처리부가 접속을 인가한 경우에, SIP 서버가, 접속원의 단말로부터의 초대 메시지를 접속처의 단말에 공급한다.

[0014] 이하에 설명한 바와 같이, 본 발명에는 다른 태양이 존재한다.

[0015] 따라서, 본 발명의 개시, 본 발명의 일부의 태양의 제공을 의도하고 있어, 여기에서 기술되어 청구되는 발명의 범위를 제한하는 것은 의도하지 않고 있다.

발명의 효과

[0016] 이상과 같이, 본 발명에 따른 감시 시스템은 통신을 사용하여 원격지에서 점포 등을 감시하기 위하여 유용하다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 감시 시스템의 전체적인 구성을 도시하는 도면.

도 2는 감시 시스템의 구성을 보다 구체적으로 도시하는 블럭도.

도 3은 본 발명의 감시 시스템에 있어서의 주요한 구성을 도시하는 블럭도.

도 4는 인가 정보 기억부에 기억되는 접속 인가 정보 테이블의 예를 나타내는 도면.

도 5는 감시 시스템에서 단말 간의 통신을 행할 때의 동작을 도시하는 도면.

도 6은 감시 장치가 접속원이 되어 단말 간의 통신을 행하는 동작을 도시하는 도면.

도 7은 이용자 장치가 접속원이 되어 단말 간의 통신을 행하는 동작을 도시하는 도면.

발명을 실시하기 위한 구체적인 내용

[0018] (발명을 실시하기 위한 형태)

[0019] 이하에 본 발명의 상세한 설명을 기술한다. 단, 이하의 상세한 설명과 첨부의 도면은 발명을 한정하는 것은 아니다.

[0020] 본 발명은, 감시 정보를 통신하는 복수의 단말과, 복수의 단말의 통신을 관리하는 통신 관리 장치를 갖고, 복수의 단말의 각각이 감시대상측 또는 감시대상으로부터 수신한 감시 정보를 이용하는 이용자측에 설치된 감시 시스템으로서, 복수의 단말중 하나가 다른 단말에 접속을 요구할 때, 이 접속원의 단말은, 접속처의 단말의 식별 정보를 포함하는 SIP의 초대 메시지를 통신 관리 장치에 송신하도록 구성되고, 통신 관리 장치는, SIP 서버와,

접속이 인가될 단말의 조합을 나타내는 접속 인가 정보를 기억한 인가 정보 기억부와, 접속 인가 정보를 참조하여 단말 간의 접속을 인가할지 아닐지를 판정하는 인가 처리부를 갖고, SIP 서버는, 접속원의 단말로부터 초대 메시지를 취득했을 때, 초대 메시지에 포함되는 접속처의 단말의 식별 정보를 인가 처리부에 공급하고, 인가 처리부가 단말 간의 접속을 인가한 경우에, SIP 서버가 접속원의 단말로부터의 초대 메시지를 접속처의 단말에 공급한다.

[0021] 상기한 바와 같이 본 발명에 의하면, 감시 시스템의 복수의 단말이 SIP 서버를 구비한 통신 관리 장치와 접속된다. 통신 관리 장치는, SIP 서버에 더하여, 접속이 인가될 단말의 조합을 나타내는 접속 인가 정보를 기억한 인가 정보 기억부와, 접속 인가 정보를 참조하여 단말 간의 접속을 인가할지 아닐지를 판정하는 인가 처리부를 갖는다. SIP의 시그널링에서는, 초대 메시지가 접속원의 단말로부터 SIP 서버로 보내진다. 이 때, 본 발명에서는, 인가 처리부가 접속을 인가할지 아닐지를 판정한다. 인가 처리부가 접속을 인가한 경우, SIP 서버가 접속원의 단말로부터의 초대 메시지를 접속처의 단말로 보내고, SIP의 시그널링이 성공한다.

[0022] 이와 같이, 본 발명에서는, 접속이 인가될 단말의 조합의 정보를 미리 기억해 두고, SIP의 시그널링 시에 단말 간의 접속의 인가를 행한다. 이것에 의해, 단말과 SIP 서버 간의 단순한 인증이 아니고, SIP 서버를 통한 단말 간 즉 P2P에 대한 인가를 행할 수 있어, 감시 정보의 이용자를 적합하게 제한할 수 있다. 이렇게 하여, 감시 시스템에 SIP를 적용하는 경우의 세큐러티성을 향상할 수 있다.

[0023] 접속처의 단말은 초대 메시지를 통신 관리 장치로부터 수신했을 때에 SIP의 OK 메시지를 통신 관리 장치에 송신해도 되고, 초대 메시지 및 OK 메시지에는, SIP 세션 확립 후에 접속원 및 접속처의 단말 간에 통신 관리 장치를 통하지 않고 단말 간 접속을 확립하기 위하여 사용되는 접속 확립 정보가 부가될 수도 있다.

[0024] 이것에 의해, SIP 세션 확립 후에, 통신 관리 장치를 통하지 않고 단말 간에 감시 정보를 통신할 수 있다. 본 발명에서는 2단계의 통신이 행해진다. 1단계째의 통신은 SIP이며, 통신 관리 장치를 통하여 행해진다. 2단계째의 통신은 통신 관리 장치를 통하지 않는 단말 간 접속이다. SIP의 접속시는 시그널링이 행해지고, 시그널링에서는 초대 메시지와 OK 메시지가 교환된다. 본 발명은, SIP의 시그널링의 메시지를 이용하여, 단말 간 접속의 확립을 위한 접속 확립 정보를 교환한다. 이렇게 하여, SIP를 능숙하게 이용하여, 단말 간 접속을 행할 수 있다. 그리고, 통신 관리 장치와 단말의 통신량을 저감하여, 통신 관리 장치의 부하를 경감할 수 있다.

[0025] 통신 관리 장치를 통하지 않는 단말 간 접속은 단말 간에 VPN을 구축하여 접속하는 단말 간 VPN일 수도 있다. 이것에 의해, 단말 간 통신(상기의 SIP 접속 후의 2단계째의 통신)에 VPN(가상 프라이빗 네트워크)을 적용함으로써 세큐러티성을 높게 할 수 있다. SIP의 시그널링에 있어서의 쌍방향의 메시지 교환이 VPN 접속 확립에 필요한 정보의 교환에 적합하게 이용된다.

[0026] 초대 메시지는 접속원의 단말의 IP 어드레스와 전자증명서를 접속 확립 정보로서 포함하고, OK 메시지는 접속처의 단말의 IP 어드레스와 전자증명서를 접속 확립 정보로서 포함할 수도 있다. 이것에 의해, SIP를 적합하게 이용하여, VPN 접속에 사용하는 정보를 교환하여, 단말 간에 안전한 통신을 행할 수 있다.

[0027] 통신 관리 장치는, 복수의 단말과의 통신을 이용하여 감시대상을 감시하는 감시 센터에 설치될 수도 있다. 이것에 의해, 통신 관리 장치를 이용하여, 감시 센터와 단말의 통신 및 단말 간의 통신을 적합하게 행할 수 있다.

[0028] 통신 관리 장치와 복수의 단말의 접속은 통신 관리 장치와 복수의 단말 사이에 VPN을 구축한 센터 단말 간 VPN에 의해 접속되어도 되고, SIP 서버는 센터 단말 간 VPN을 통하여 복수의 단말과 SIP 메시지를 통신할 수도 있다. 이것에 의해 SIP 통신이 센터 단말 간 VPN상에서 행해진다. 상기에서는, SIP 세션 확립 후에, 단말 간에 VPN 접속을 행하는 것을 기술했다. 여기에서의 센터 단말 간 VPN은 센터와 각각의 단말 사이의 VPN이다. 센터 단말 간 VPN을 사용함으로써, 감시 센터와 각 단말의 통신의 세큐러티를 확보할 수 있고, 그리고, SIP 통신의 세큐러티도 확보할 수 있다.

[0029] 감시 정보는 감시대상에서 촬영된 화상, 감시대상에서 검출된 감시 신호, 이용자측에서 생성된 제어 정보 중 적어도 하나를 포함할 수도 있다. 이것에 의해, 단말 간에 유용한 감시 정보를 통신할 수 있다.

[0030] 본 발명의 다른 태양은 감시 정보를 통신하는 복수의 단말의 통신을 관리하는 통신 관리 장치이다. 이 통신 관리 장치는 SIP 서버와, 접속이 인가될 단말의 조합을 나타내는 접속 인가 정보를 기억한 인가 정보 기억부와, 접속 인가 정보를 참조하여 단말 간의 접속을 인가할지 아닐지를 판정하는 인가 처리부를 갖고, SIP 서버가 복수의 단말 중 하나로부터, 다른 단말로의 식별 정보를 포함하는 SIP의 초대 메시지를 취득했을 때, 인가 처리부가, 초대 메시지에 포함되는 접속처의 단말의 식별 정보에 기초하여, 단말 간의 접속을 인가할지 아닐지를 판정

하고, 인가 처리부가 접속을 인가한 경우에, SIP 서버가 접속원의 단말로부터의 초대 메시지를 접속처의 단말에 공급한다. 이 태양에도 상기의 각종 구성이 적용될 수도 있다.

[0031] 본 발명은 상기 감시 시스템 및 통신 관리 장치의 태양에 한정되지 않는다. 본 발명의 다른 태양은, 예를 들면, 단말 장치이다. 또한 본 발명은 방법, 프로그램, 또는 동 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체의 형태로 실현될 수도 있다.

[0032] 전술한 바와 같이, 본 발명은 감시 시스템에 SIP를 적용하는 경우의 세큐러티를 향상할 수 있다.

[0033] 이하, 본 발명의 실시형태의 감시 시스템에 대하여, 도면을 사용하여 설명한다.

[0034] 도 1은 본 발명의 감시 시스템의 전체적인 구성을 도시하고 있다. 도시된 바와 같이, 감시 시스템(1)에서는, 감시 센터(3), 감시대상(5) 및 이용자 거점(7) 간에 통신이 행해진다. 여기에서 이용자란 감시 시스템(1)에 의한 감시대상(5)의 감시 서비스의 이용자를 의미한다. 본 실시형태의 예에서는, 감시대상(5)이 점포이며, 이용자 거점(7)은 점포의 오너의 사무소이다.

[0035] 감시 센터(3)에는 통신 관리 장치(11) 및 복수의 센터 장치(13)가 구비되어 있고, 이것들은 통신 가능하게 접속되어 있다. 통신 관리 장치(11) 및 복수의 센터 장치(13)는 지리적으로는 떨어진 장소에 배치될 수도 있다. 복수의 센터 장치(13)는 복수의 담당지역에 각각 배치될 수도 있다. 또한 복수의 센터 장치(13)는 기능을 분담할 수도 있다. 예를 들면, 어떤 센터 장치(13)가 경비 관련의 신호를 처리하는 관제 센터 장치로서 기능할 수도 있고, 다른 센터 장치(13)가 감시 영상을 주로 처리하는 화상 센터 장치로서 기능할 수도 있다. 또한, 본 발명의 범위에서 센터 장치(13)가 하나일 수도 있다.

[0036] 감시대상(5) 및 이용자 거점(7)에는, 각각, 감시 장치(15) 및 이용자 장치(17)가 설치되어 있다. 감시 장치(15) 및 이용자 장치(17)는 본 발명의 단말에 상당한다. 감시 장치(15)는 감시 정보를 센터 장치(13) 및 이용자 장치(17)에 보낸다. 감시 정보는, 예를 들면, 감시 카메라의 화상이며, 또한 감시대상(5)에서 검출된 감시 신호이다. 감시 신호는, 예를 들면 이상 발생을 나타내는 경비 신호이며, 경비 신호는 감시대상(5)에 설치된 센서로부터의 검출 신호에 기초하여 생성되거나, 또는, 경보 버튼(스위치)이 조작되었을 때에 생성된다. 또한 이용자 장치(17)는 감시 장치(15)에 제어 신호나, 음성 신호를 보낸다. 이러한 이용자 장치(17)로부터 감시 장치(15)로의 신호도, 감시 정보에 포함된다.

[0037] 도 1에서는, 1개의 감시대상(5) 및 1개의 이용자 거점(7)이 도시되어 있다. 그러나, 실제로는, 감시 센터(3)는 복수의 감시대상(5) 및 복수의 이용자 거점(7)과 통신한다. 따라서, 통신 관리 장치(11)도 복수의 감시 장치(15) 및 복수의 이용자 장치(17)와 통신한다. 각각의 감시 장치(15)는 관련지어진 이용자 장치(17)(점포의 오너의 단말)과 통신한다.

[0038] 도 1의 감시 시스템(1)에 의하면, 예를 들면, 감시 장치(15)가 센서 신호 등에 의해 이상을 검출했다고 가정한다. 이 경우, 감시 정보로서 경비 신호가 감시대상(5)의 영상과 함께, 감시 센터(3)에 송신된다. 감시 센터(3)에서는, 오퍼레이터가 센터 장치(13)의 모니터에서 경비 신호나 영상을 확인하고, 경비원에게 필요한 지시를 내린다. 지시를 받은 경비원이 감시대상(5)으로 급행하여, 이상에 대처한다.

[0039] 또 예를 들면, 감시 장치(15)는 감시대상(5)의 영상 등을 정기적으로, 또는 그 밖의 설정에 따라 이용자 장치(17)에 보낸다. 예를 들면, 센서에 의해 손님이 검출되었을 때, 영상 등이 이용자 장치(17)에게 보내진다. 또한 이용자 장치(17)로부터 영상 등의 송신이 요구되는 경우도 있다. 오너는, 영상 등에 의해 점포의 모습을 파악할 수 있다. 또한 오너는 이용자 장치(17)로부터 감시 장치(15)에 음성 등을 보내어, 점원에게 필요 사항을 지시할 수 있다.

[0040] 다음에 감시 시스템(1)의 통신 형태에 대하여 설명한다. 통신 관리 장치(11), 감시 장치(15) 및 이용자 장치(17)는 인터넷에 접속되어 있다.

[0041] 또한, 통신 관리 장치(11)는 인터넷상에서 센터 단말 간 VPN(가상 프라이빗 네트워크)(21)에 의해 감시 장치(15) 및 이용자 장치(17)와 접속된다. 센터 단말 간 VPN(21)을 구축하기 위하여, 통신 관리 장치(11)에 VPN 서버 기능이 구비되고, 감시 장치(15) 및 이용자 장치(17)에 VPN 클라이언트 기능이 구비된다. VPN에서는 VPN 터널이 구축되고, 암호화 통신이 행해져, 높은 세큐러티성이 실현된다.

[0042] 또한 감시 장치(15)와 이용자 장치(17)는 통신 관리 장치(11)를 통하여 SIP 통신(23)을 행한다. SIP 통신(23)은 상기의 센터 단말 간 VPN(21)을 통하여 행해진다. 통신 관리 장치(11)에는 SIP 서버 기능이 구비되어 있다.

[0043] 또한 감시 장치(15)와 이용자 장치(17)는 통신 관리 장치(11)를 통하지 않고, 직접적으로 단말 간 VPN(25)에 의해 접속된다. 이 단말 간 VPN(25)을 구축하기 위하여, 이용자 장치(17)에 VPN 서버 기능이 구비되고, 감시 장치(15)에 VPN 클라이언트 기능이 구비된다.

[0044] 여기에서, 센터 단말 간 VPN(21)은 항상 접속되어 VPN 터널이 구축되어 있고, 센터 장치(13)와 감시 장치(15) 및 이용자 장치(17) 사이에서의 통신에 이용된다. 이것에 대하여, 단말 간 VPN(25)은 필요할 때만 구축된다.

[0045] 단말 간 VPN(25)을 사용하는 이유를 설명한다. 감시 시스템(1)에서는 영상 등의 대용량의 데이터가 통신된다. 센터 단말 간 VPN(21)이 모든 통신에 사용되면, 통신 관리 장치(11)의 부하가 팽대하게 된다. 그래서, 감시 장치(15)와 이용자 장치(17)의 통신을 단말 간 VPN(25)에 의해 행함으로써, 세큐러티성을 확보하면서, 통신 관리 장치(11)의 부하를 경감하고 있다.

[0046] 또한, 본 실시형태에 있어서의 SIP 통신(23)의 역할은 일반적인 IP 전화 등과는 상이한 특별한 것이다. 즉, 본 실시형태는 SIP의 시그널링을 VPN 접속전의 준비의 처리로서 자리 매기고 있다. 보다 상세하게는, SIP(23)의 세션을 확립할 때에는, 시그널링이 행해진다. 이 시그널링으로 쌍방향 통신이 행해지고, 초대 메시지와 OK 메시지가 교환된다. 한편, VPN 접속을 확립하기 위해서는, 정보의 교환이 필요하다. 본 실시형태에서는, IP 어드레스 및 전자증명서가 교환된다. 전자증명서는 전자서명 등의 정당성을 검증할 때에 이용되고, 신뢰가 있는 제3자 기관으로부터 발행되는 것을 사용한다. 그래서, SIP 통신(23)의 시그널링이 VPN 접속 확립을 위한 정보 교환의 수단으로서 이용된다.

[0047] 이상으로, 감시 시스템(1)의 전체 구성을 설명했다. 상기한 바와 같이, 본 실시형태에서는, 2종류의 VPN이 사용된다. 한쪽은 통신 관리 장치(11)와 단말(감시 장치(15) 또는 이용자 장치(17))을 접속하고, 다른 한쪽은 단말끼리(감시 장치(15)와 이용자 장치(17))를 접속한다. 그래서, 도 1에서는, 이들 2개의 VPN을 구별하기 위하여, 센터 단말 간 VPN(21)과 단말 간 VPN(25)과 같은 용어를 사용하고 있다. 단, 단지 VPN(21), VPN(25)과 같은 용어가 사용될 수도 있다.

[0048] 다음에 도 2를 참조하여 감시 시스템(1)의 구성을 보다 구체적으로 설명한다. 통신 관리 장치(11)는 방화벽(31), HTTP 서버(33), VPN 서버(35), SIP 서버(37), STUN 서버(39), 어카운트 관리 서버(41), 데이터 베이스(43) 및 로그 서버(45)를 구비한다.

[0049] 방화벽(31)은 통신 관리 장치(11)와 감시 장치(15) 및 이용자 장치(17) 사이에서 사용되는 통신 데이터 이외의 데이터를 차단하는 장치이다. HTTP 서버(33)는 인터넷 접속을 위한 구성이다. VPN 서버(35)는 VPN 터널 구축을 위한 인증과 암호화를 행하는 서버이다.

[0050] VPN 서버(35)는 센터 단말 간 VPN(21)을 실현하는 구성이며, 통신 관리 장치(11)와 감시 장치(15) 사이에 VPN을 구축하고, 또한 통신 관리 장치(11)와 이용자 장치(17) 사이에 VPN을 구축한다. 감시 장치(15)로부터의 신호는 VPN 서버(35)에서 복호화되어, 센터 장치(13)에 송신된다. 또한 센터 장치(13)로부터의 신호는 VPN 서버(35)에서 암호화되어, 감시 장치(15)에 송신된다. 또한 통신 관리 장치(11)가 감시 장치(15)에 신호를 보낼 때도, VPN 서버(35)에서 암호화가 행해진다. 통신 관리 장치(11)와 이용자 장치(17)의 통신에서도, VPN 서버(35)가 마찬가지로 암호화 및 복호화를 행한다.

[0051] SIP 서버(37)는 SIP 프로토콜에 따라 시그널링의 처리를 행하고, 감시 장치(15)와 이용자 장치(17)를 접속한다. SIP 서버(37)는, 이용자 장치(17)가 감시 장치(15)에 접속을 요구하는 경우에, 혹은, 감시 장치(15)가 이용자 장치(17)에 접속을 요구하는 경우에, SIP의 접속 제어의 기능을 수행한다.

[0052] SIP의 시그널링에서는 메시지가 교환된다. 구체적으로는, INVITE(초대) 메시지와 OK 메시지가 교환된다. 이 메시지 교환을 이용하여, 전술한 바와 같이, VPN 접속 확립을 위해 IP 어드레스 및 전자증명서가 교환된다.

[0053] STUN 서버(39)는 감시 장치(15) 및 이용자 장치(17)의 라우터의 NAT 기능에 대응하기 위하여 STUN 기능을 제공한다.

[0054] 어카운트 관리 서버(41)는 인증 등의 각종 정보를 관리하는 서버이다. 관리되는 정보는 데이터 베이스(43)에 저장된다. 관리되는 정보는 IP 회선의 어카운트, VPN 접속(터널 구축)을 위한 전자증명서, 키 페어의 정보를 포함한다. 또한 본 실시형태에서는, SIP의 시그널링의 과정에서, 단말 간의 접속에 대하여 인증 및 인가가 행해진다. 이 처리를 위한 정보도 데이터 베이스(43)에 유지되고, 어카운트 관리 서버(41)에 사용된다. 또한,

단말 간의 접속에 대한 인증 및 인가는 SIP 서버 자신이 행하도록 할 수도 있고, 이 경우에는 본 발명의 인가 처리부 및 인가 정보 기억부가 SIP 서버에 구비되게 된다.

[0055] 로그 서버(45)는 감시 장치(15)에서 생성한 로그을 보존하기 위한 서버이다.

[0056] 센터 장치(13)는 감시 테이블(51)과 회선 접속 장치(53)를 구비한다. 감시 테이블(51)이 회선 접속 장치(53)를 통하여 통신 관리 장치(11)에 접속된다. 예를 들면, 센터 장치(13)가 화상 센터인 경우, 감시 영상이 감시 테이블(51)에 공급되고, 감시 테이블(51)에서 관리된다. 또한 센터 장치(13)가 관제 센터인 경우, 경비 관련의 정보가 감시 테이블(51)에 공급된다. 감시 영상도 관제 센터의 모니터에 적합하게 표시된다. 감시 영상 등은 센터 장치끼리의 사이에서도 통신될 수도 있다.

[0057] 다음에, 감시 장치(15)에 대하여 설명한다. 감시 장치(15)는 컨트롤러(61), IP 회선 유닛(63), 라우터(65), 주변기기(67), 멀티 회선 어댑터(69) 및 감시대상 PC(퍼스널 컴퓨터)(71)로 구성되어 있다.

[0058] 컨트롤러(61)는 컴퓨터로 구성되어 있고, 주변기기(67)와 연계하여, 감시기능을 실현한다. 컨트롤러(61)는 감시 센터(3)와는 IP 회선 유닛(63)을 통하여 접속된다. 또한 컨트롤러(61)는 이용자 장치(17)와도 IP 회선 유닛(63)을 통하여 접속된다.

[0059] 도 2에서는, 주변기기(67)로서 감시 카메라(73), 센서(75) 및 경보 버튼(77)이 예시되어 있다. 컨트롤러(61)는 감시 영상에 대하여 화상 인식 처리를 시행하여 이상을 검출한다. 또한 컨트롤러(61)는 센서(75)로부터 입력되는 검출 신호에 의해 이상을 검출한다. 경보 버튼(77)이 눌려졌을 때에도 이상이 검출된다. 그 밖의 주변기기가 이상 검출에 사용될 수도 있다. 이상이 발생하면, 컨트롤러(61)는 센터 장치(13)와 통신하고, 경비 신호와 화상 신호를 송신한다. 감시 카메라(73)와 함께 마이크가 구비되어 있고, 음성 신호도 송신된다. 이렇게 하여, 컨트롤러(61)는 감시대상(5)의 경비 기능을 실현한다.

[0060] 또한, 감시 영상 및 음성은 센터 장치(13)로부터 요구되었을 때에도 송신된다. 또한, 감시 영상 및 음성은 이용자 장치(17)에도 보내진다. 이용자 장치(17)로의 송신은, 예를 들면, 정기적으로 행해지고, 또한 그 밖의 설정에 따라서 행해진다. 예를 들면, 센서(75)에 의해 손님이 검지되면, 영상 등이 이용자 장치(17)에 보내진다. 또한 이용자 장치(17)로부터 요구되었을 때도, 감시 장치(15)는 영상 등을 송신한다.

[0061] IP 회선 유닛(63)은 컨트롤러(61)가 통신 관리 장치(11)와 통신하기 위한 VPN 터널을 구축한다. 또한 컨트롤러(61)가 이용자 장치(17)와 통신하기 위한 VPN 터널을 구축한다. 전자는 센터 단말 간 VPN(21)에 대응하고, 후자는 단말 간 VPN(25)에 대응한다. 이것들의 접속에 있어서, IP 회선 유닛(63)은 VPN 클라이언트의 기능을 실현한다.

[0062] 도 2에서는, IP 회선 유닛(63)이 컨트롤러(61)의 내부 구성으로서 도시되어 있다. 이것은 물리적인 배치를 표현하고 있다. 통신 구성으로서는 IP 회선 유닛(63)은 컨트롤러(61)와 라우터(65) 사이에 배치되어 있다. 그리고, IP 회선 유닛(63)은 컨트롤러(61)와 이더넷(등록상표)으로 LAN 접속되어 있다. 라우터(65)는 브로드밴드 회선용의 라우터이다.

[0063] 멀티 회선 어댑터(69)는 휴대전화망을 통하여 센터 장치(13)와 접속된다. 멀티 회선 어댑터(69)는 브로드밴드 회선이 불통일 때에 경비 신호를 송신하기 위하여 사용된다. 경비 신호가 컨트롤러(61)로부터 IP 회선 유닛(63)을 통하여 멀티 회선 어댑터(69)에 보내지고, 멀티 회선 어댑터(69)로부터 센터 장치(13)에 송신된다.

[0064] 감시대상 PC(71)는 감시대상(5)에 설치되는 PC이다. 본 실시형태의 예에서는 감시대상(5)이 점포이다. 따라서, 감시대상 PC(71)는 점포용의 PC일 수도 있다.

[0065] 다음에, 이용자 장치(17)에 대하여 설명한다. 이용자 장치(17)는 VPN 종단 장치(이하, VTE)(81), 라우터(83) 및 이용자 PC(퍼스널 컴퓨터)(85)로 구성되어 있다.

[0066] VTE(81)는 브로드밴드 접속을 위한 회선 종단 장치이다. 그리고, VTE(81)는 통신 관리 장치(11)의 VPN 서버(35)와 VPN 터널을 구축하고, 또한 감시 장치(15)의 IP 회선 유닛(63)과 VPN 터널을 구축한다. 전자에서는 VTE(81)가 VPN 클라이언트로서 기능하고, 후자에서는 VTE(81)가 VPN 서버로서 기능한다. 라우터(83)는 브로드밴드 회선용의 라우터이다.

[0067] VTE(81)는 이용자 PC(85)와 접속된다. VTE(81)는 감시 장치(15)의 컨트롤러(61)로부터 수신한 영상, 음성 및 제어 신호를 이용자 PC(85)에 전송한다. 또한 VTE(81)는 이용자 PC(85)로부터 수신한 음성 및 제어 신호를 컨트롤러(61)에 전송한다.

[0068] 본 실시형태에서는, 이용자 거점(7)이 점포의 오너의 사무소 등이다. 따라서, 이용자 PC(85)는 점포의 오너의 PC일 수도 있다. 이용자 PC(85)는 오너가 감시대상(5)의 감시 영상을 보기 위해서 사용된다. 이 기능을 제공하기 위하여, 이용자 PC(85)에는, 컨트롤러(61)와 통신함으로써 감시대상(5)의 감시 영상을 표시 및 전환할 수 있는 어플리케이션 소프트웨어가 인스톨되어 있다.

[0069] 본 실시형태에서는 이용자 장치(17)가 고정되어 있다. 그러나, 이용자 장치(17)의 기능이 휴대단말 등에 넣어져서, 이동 가능할 수도 있다.

[0070] 이상으로 감시 시스템(1)의 전체적인 구성을 설명했다. 다음에 본 발명의 특징에 따른 구성에 대하여 설명한다.

[0071] 도 3은 도 1 및 도 2에 도시된 감시 시스템(1)의 일부로서, 본 발명의 주요한 부분을 도시하고 있다. 도 3에 있어서, 도 1 및 도 2에서 설명된 요소에는, 동일한 부호가 첨부되어 있다.

[0072] 도 3에 도시하는 바와 같이, 통신 관리 장치(11)는 VPN 서버(35), SIP 서버(37)에 더하여, 인가 정보 기억부(101) 및 인가 처리부(103)를 구비하고 있다. 인가 정보 기억부(101)는 접속이 인가될 단말(감시 장치(15) 및 이용자 장치(17))의 조합을 나타내는 접속 인가 정보를 기억한다. 그리고, 인가 처리부(103)는 접속 인가 정보를 참조하여 단말 간의 접속을 인가할지 아닐지를 판정한다. 인가 정보 기억부(101) 및 인가 처리부(103)는 도 2의 데이터 베이스(43) 및 어카운트 관리 서버(41)에 의해 각각 실현된다.

[0073] 도 4는 인가 정보 기억부(101)에 기억될 접속 인가 정보의 예를 도시하고 있다. 이 예에서는, 접속 인가 정보가 단말 ID의 조합을 나타내는 테이블이다. 이 테이블은 각 이용자(점포의 오너)와, 감시 장치 ID(감시 장치(15)의 ID)와, 이용자 장치 ID(이용자 장치(17)의 ID)를 대응시키고 있다. 감시 장치 ID 및 이용자 장치 ID는 감시 장치(15) 및 이용자 장치(17)를 특정 가능한 임의의 정보일 수도 있다. 후술의 예에서는, 감시 장치 ID가 IP 회선 유닛(63)의 ID이며, 이용자 장치 ID가 VTE(81)의 ID이다.

[0074] 한 사람의 오너가 복수의 점포를 갖는 경우가 있다. 이 경우, 하나의 감시 장치(15)가 복수의 이용자 장치(17)와 조합된다. 도 4의 예에서는, 이용자(C)가 2개의 점포를 갖고 있고, 2개의 감시 장치(15(C01, C02))가 이용자 장치(17(C11))와 대응시켜져 있다. 그 밖에, 한 사람의 오너가 복수의 이용자 장치(17)를 사용하는 경우 등은, 하나의 감시 장치(15)가 복수의 이용자 장치(17)와 대응시켜질 수도 있다.

[0075] 도 3으로 되돌아와, 감시 장치(15)에 있어서, IP 회선 유닛(63)은 SIP 처리부(111), VPN 처리부(113) 및 기억부(115)를 갖는다. SIP 처리부(111) 및 VPN 처리부(113)는, 각각, SIP 및 VPN에 관한 처리를 행한다. 기억부(115)는 IP 회선 유닛(63)에서 처리되는 각종 정보를 기억한다. 특히, 본 발명에 관련하여, 기억부(115)는 IP 회선 유닛(63)의 IP 어드레스와 전자증명서를 기억하고 있다. 이들 정보는 본 발명의 접속 확립 정보에 상당하고, VPN 접속을 위해 접속 상대로 제공된다. 또한 기억부(115)는, IP 회선 유닛 ID(IP 회선 유닛(63)의 ID)를 기억하고 있고, 이 IP 회선 유닛 ID가 감시대상(5)의 ID로서 사용된다.

[0076] 도 3에 도시하는 바와 같이, 이용자 장치(17)의 VTE(81)도 SIP 처리부(121), VPN 처리부(123) 및 기억부(125)를 가지고 있다. 기억부(125)는 VTE(81)의 IP 어드레스와 전자증명서를 기억하고 있다. 또한 기억부(125)는 VTE-ID(VTE(81)의 ID)를 기억하고 있다.

[0077] 다음에 본 실시형태의 동작을 설명한다. 여기에서는, 단말 간 VPN(25)을 구축할 때의 동작, 즉, 감시 장치(15)와 이용자 장치(17) 간의 VPN 접속을 행할 때의 동작을 설명한다.

[0078] 우선, 동작의 개요를 설명한다. 이미 설명한 바와 같이, 통신 관리 장치(11)와 감시 장치(15) 사이에는, 센터 단말 간 VPN(21)이 항상 구축되어 있다. 통신 관리 장치(11)와 이용자 장치(17) 사이에도 센터 단말 간 VPN(21)이 항상 구축되어 있다. 이들 센터 단말 간 VPN(21)과는 별도로, 이하의 동작에 의해, 감시 장치(15)와 이용자 장치(17) 간에 직접적으로 단말 간 VPN(25)이 구축된다.

[0079] 단말 간 VPN(25)을 접속할 때에는 정보의 교환이 행해진다. 본 실시형태에서는, IP 어드레스와 전자증명서가 감시 장치(15)와 이용자 장치(17) 사이에서 교환된다. 이 정보 교환의 수단으로서 본 실시형태는 SIP에 주목하고 있다. SIP의 시그널링에서는, 단말 간에 메시지가 교환된다. 이들 SIP 메시지에 상기의 IP 어드레스 및 전자증명서가 넣어진다. 이것에 의해, SIP의 시그널링 과정에서, 단말 간 VPN(25)의 구축 준비를 위한 정보 교환을 행할 수 있다.

[0080] SIP의 기본적 기능에서는 SIP 서버(37)에 등록되어 있는 임의의 어드레스 간에 SIP의 접속이 확립된다. 이 경우, 감시 장치(15)가 관계없는 이용자 장치(17)와 접속될 가능성이 있어, 세큐러티상 바람직하지 않다. 이 점

을 배려하여, 본 실시형태에서는, 이하와 같이 하여 시그널링이 행해진다. 이하에서는, 감시 장치(15) 및 이용자 장치(17)의 일방을 SIP의 접속원 단말로 하고, 타방을 SIP의 접속처 단말로 한다. 또한 SIP의 메시지는 센터 단말 간 VPN(21)상에서 송신된다.

[0081] 도 5를 참조하면, 우선, 접속원 단말이 INVITE 메시지(상세하게는 SIP INVITE 메시지, 이하 동일)를 SIP 서버(37)에 보낸다(S1). INVITE 메시지에는, 접속원 단말의 ID 및 접속처 단말의 ID와, 접속원 단말의 IP 어드레스 및 전자증명서가 부가된다.

[0082] SIP 서버(37)는, INVITE 메시지를 받으면, 접속원 단말의 ID와 접속처 단말의 ID를 인가 처리부(103)에 공급하고, 그들 접속원 단말과 접속처 단말의 접속의 가부를 인가 처리부(103)에 문의한다(S3). 인가 처리부(103)는 인가 정보 기억부(101)의 접속 인가 정보를 참조하여, 접속을 인가할지 아닐지의 판정을 행한다(S5). 접속원 단말과 접속처 단말의 조합이 인가 정보 기억부(101)에 등록되어 있으면, 접속이 인가된다.

[0083] SIP 서버(37)는 인가 처리부(103)로부터 인가 결과를 받는다(S7). SIP 서버(37)는 인가 처리부(103)에 의해 접속이 인가되면, INVITE 메시지를 접속처 단말에 송신한다(S9). 이 INVITE 메시지는 접속원 단말의 IP 어드레스 및 전자증명서를 포함한다.

[0084] 접속처 단말은, INVITE 메시지를 수신하면, SIP 서버(37)에 OK 메시지(상세하게는 SIP 2000 OK 메시지, 이하, 동일)를 보낸다(S11). OK 메시지에는, 접속처 단말의 IP 어드레스와 전자증명서가 부가된다. 이 OK 메시지가 SIP 서버(37)를 통하여 접속원 단말에 송신된다(S13). 이렇게 하여, SIP의 시그널링에 의해 IP 어드레스 및 전자증명서가 교환된다. 그리고, 단말 간에 VPN을 구축하려고 할 때는, 접속 요구에 포함되는 전자증명서와 먼저 교환한 전자증명서에 의해 인증을 행하고, 단말 간 VPN(25)이 구축된다(S15).

[0085] 전술한 바와 같이, 본 실시형태에서는, INVITE 메시지가 SIP 서버(37)에 수신되었을 때에, 단말의 조합을 인가하는 처리가 행해진다. 접속이 인가되지 않으면, INVITE 메시지는 접속처 단말에 보내지지 않고, 그 후의 SIP의 처리도 VPN의 처리도 행해지지 않는다. 감시 장치(15)와 이용자 장치(17)의 조합이 적정한 경우만, 접속이 인가되어, INVITE 메시지가 접속처 단말에 보내지고, 그 후의 SIP의 처리가 행해져, 최종적으로 VPN 접속이 가능하다.

[0086] 다음에 도 6 및 도 7을 참조하여, 감시 시스템(1)의 동작의 상세를 설명한다. 여기에서는, 우선, 감시 장치(15)가 접속원 단말일 경우에 대하여 설명하고, 다음에 이용자 장치(17)가 접속원일 경우에 대하여 설명한다.

[0087] 도 6의 타임 차트에 있어서, 컨트롤러(61) 및 IP 회선 유닛(63)이 감시 장치(15)의 구성이며, SIP 서버(37) 및 인가 정보 기억부(101)(어카운트 관리 서버(41))가 통신 관리 장치(11)의 구성이며, VTE(81) 및 이용자 PC(85)가 이용자 장치(17)의 구성이다.

[0088] 컨트롤러(61)는 VTE-ID(VTE(81)의 ID)를 포함하는 접속 지시(P2P 접속 지시)를 IP 회선 유닛(63)에 보낸다(S101). 여기에서는, VTE-ID가 접속처 단말 ID로서 사용되고 있다.

[0089] IP 회선 유닛(63)은 기억부(115)로부터 IP 회선 유닛 IP 어드레스(IP 회선 유닛(63)의 IP 어드레스) 및 IP 회선 유닛 개별증명서를 읽어낸다. IP 회선 유닛 개별증명서는 IP 회선마다 배정된 전자증명서이다. 또한 IP 회선 유닛(63)은, 기억부(115)로부터, 접속원 단말 ID로서의 IP 회선 유닛 ID(IP 회선 유닛(63)의 ID)를 읽어낸다. 그리고, IP 회선 유닛(63)은, 이들 정보를 INVITE 메시지에 부가하여, INVITE 메시지를 SIP 서버(37)에 보낸다(S103). 구체적으로는, INVITE 메시지는, IP 회선 유닛 IP 어드레스, IP 회선 유닛 ID, VTE-ID 및 IP 회선 유닛 개별증명서를 포함한다.

[0090] SIP 서버(37)는, INVITE 메시지를 수신하고, IP 회선 유닛 ID 및 VTE-ID를 인가 처리부(103)에 알리고, 접속을 인가할지 아닐지를 문의한다(S105). 인가 처리부(103)는, 인가 정보 기억부(101)의 접속 인가 정보를 참조하여, 접속을 인가할지 아닐지를 판정한다(S107). 여기에서는, 도 4의 테이블이 읽어 내진다. 그리고, 인가 처리부(103)는 문의의 단말 ID의 조합이 테이블에 등록되어 있는지 아닌지를 판정한다. 해당하는 조합이 등록되어 있으면, 인가 처리부(103)는 접속을 인가한다. 인가 결과는 인가 처리부(103)로부터 SIP 서버(37)로 전해진다(S109). SIP 서버(37)는, 인가 처리부(103)가 접속을 인가한 경우에, INVITE 메시지를 VTE(81)에 송신한다(S111). 이 INVITE 메시지에는, IP 회선 유닛 IP 어드레스 및 IP 회선 유닛 개별증명서가 부가된다.

[0091] 상기의 처리에 있어서, 스텝 S107에서 접속이 인가되지 않으면, SIP 서버(37)는 INVITE 메시지를 VTE(81)로 보내지 않는다. 따라서, 그 후의 SIP의 처리는 행해지지 않고, 또한 그 후의 VPN 접속도 행해지지 않는다.

[0092] VTE(81)는, INVITE 메시지를 수신하면, IP 회선 유닛 IP 어드레스 및 IP 회선 유닛 개별증명서를 기억부(125)에 유지하고, 이용자 PC(85)에 접속 요구(P2P 접속 요구)의 문의를 행한다(S113). 이 접속 요구에는, IP 회선 유닛 IP 어드레스가 부가된다. 그리고, 이용자 PC(85)가 VTE(81)에 접속 응답을 보낸다(S115).

[0093] VTE(81)는 VTE-IP 어드레스(VTE(81)의 IP 어드레스) 및 VTE 개별증명서(VTE(81)에 배정된 전자증명서)를 기억부(125)로부터 읽어낸다. 그리고, VTE(81)는 OK 메시지를 SIP 서버(37)에 송신한다(S117). 이 OK 메시지에는, VTE-IP 어드레스, VTE 개별증명서가 부가된다.

[0094] SIP 서버(37)는 VTE-IP 어드레스 및 VTE 개별증명서와 함께 OK 메시지를 IP 회선 유닛(63)에 송신한다(S119). IP 회선 유닛(63)은, OK 메시지를 수신하면, VTE-IP 어드레스 및 VTE 개별증명서를 기억부(115)에 유지하고, ACK 메시지를 SIP 서버(37)에 보내고(S121), 또한 SIP 서버(37)가 ACK 메시지를 VTE(81)에 보낸다(S123).

[0095] 상기의 과정에서, IP 회선 유닛(63)은 VTE(81)의 IP 어드레스 및 전자증명서를 취득하고 있다. 또한 VTE(81)는 IP 회선 유닛(63)의 IP 어드레스 및 전자증명서를 취득하고 있다. 따라서, 이들 정보를 사용하여 상대방을 인식하고 IP 회선 유닛(63)과 VTE(81) 간에 VPN 접속 확립이 가능하게 된다. 이것이, 단말 간 VPN(25)이다.

[0096] 도시된 바와 같이, IP 회선 유닛(63)이 VTE(81)에 VPN 접속 요구를 행한다(S125). 여기에서는, SIP 서버(37)를 통하지 않고, 직접적으로 VPN 접속이 요구된다. VTE(81)는 VPN 접속 요구에 포함되는 IP 회선 유닛 개별증명서와 기억부(125)에 유지되어 있는 IP 회선 유닛의 개별증명서에 의해 인증을 행하고, 상대편의 IP 회선 유닛 IP 어드레스를 포함하는 착신 정보를 이용자 PC(85)에 보낸다(S127). IP 회선 유닛 IP 어드레스는 이용자 PC(85)에서 VPN 통신을 위해 사용된다. 또한 VTE(81)는 VPN 서버로서 VPN 접속의 처리를 행한 것을 IP 회선 유닛(63)에 통지한다(S129). IP 회선 유닛(63)은 접속결과가 OK인 것을 컨트롤러(61)에 통지하고, 또 상대편의 VTE-IP 어드레스를 컨트롤러(61)에 통지한다(S131). VTE-IP 어드레스는 컨트롤러(61)에서 VPN 통신을 위해 사용된다. 이렇게 하여, VPN 접속이 확립되어 단말 간 VPN(25) 을 통하여 정보가 통신된다. 감시 영상 및 음성 등이 감시 장치(15)로부터 이용자 장치(17)에 제공된다.

[0097] 다음에, 도 7을 참조하여, 이용자 장치(17)가 접속원인 경우에 대하여 설명한다. 이용자(오너)가, 예를 들면, 영상표시의 지시를 이용자 PC(85)에 입력했다고 가정한다. 이용자 PC(85)는 IP 회선 유닛 ID를 포함하는 접속 지시(P2P 접속 지시)를 VTE(81)에 보낸다(S201). 여기에서는, IP 회선 유닛 ID가 접속처 단말의 ID로서 사용되고 있다.

[0098] VTE(81)는 기억부(125)로부터 VTE-IP 어드레스 및 VTE 개별증명서를 읽어낸다. 또한 VTE(81)는, 기억부(125)로부터, 접속원 단말 ID로서의 VTE-ID를 읽어낸다. 그리고, VTE(81)는 이들 정보를 INVITE 메시지에 부가하고, INVITE 메시지를 SIP 서버(37)에 보낸다(S203). 구체적으로는, INVITE 메시지는 VTE-IP 어드레스, VTE-ID, IP 회선 유닛 ID 및 VTE 개별증명서를 포함한다.

[0099] SIP 서버(37)는 INVITE 메시지를 수신하고, VTE-ID, IP 회선 유닛 ID를 인가 처리부(103)에 알리고, 접속을 인가할지 아닐지를 문의한다(S205). 인가 처리부(103)는 상기와 동일하게 하여 인가 정보 기억부(101)의 접속 인가 정보를 참조하고, 접속을 인가할지 아닐지를 판정하고(S207), 인가 결과를 SIP 서버(37)에 전달한다(S209). 즉, VTE-ID, IP 회선 유닛 ID의 조합이 등록되어 있으면, 접속이 인가된다. SIP 서버(37)는, 인가 처리부(103)가 접속을 인가한 경우에, INVITE 메시지를 IP 회선 유닛(63)에 송신한다(S211). 이 INVITE 메시지에는 VTE-IP 어드레스 및 VTE 개별증명서가 부가된다.

[0100] 상기의 처리에 있어서, 스텝 S207에서 접속이 인가되지 않으면, SIP 서버(37)는 INVITE 메시지를 IP 회선 유닛(63)으로 보내지 않는다. 따라서, 그 후의 SIP의 처리는 행해지지 않고, 또한 그 후의 VPN 접속도 행해지지 않는다.

[0101] IP 회선 유닛(63)은, INVITE 메시지를 수신하면, VTE-IP 어드레스 및 VTE 개별증명서를 기억부(115)에 유지한다. 또한 IP 회선 유닛(63)은 컨트롤러(61)에 접속 요구(P2P 접속 요구)의 문의를 행한다(S213). 이 접속 요구에는 VTE-IP 어드레스가 부가된다. 그리고, 컨트롤러(61)가 IP 회선 유닛(63)에 접속 응답을 보낸다(S215).

[0102] IP 회선 유닛(63)은 IP 회선 유닛 IP 어드레스 및 IP 회선 유닛 개별증명서를 기억부(115)로부터 읽어낸다. 그리고. IP 회선 유닛(63)은, OK 메시지를 SIP 서버(37)에 송신한다(S217). 이 OK 메시지에는 IP 회선 유닛 IP 어드레스, IP 회선 유닛 개별증명서가 부가된다.

[0103] SIP 서버(37)는 IP 회선 유닛 IP 어드레스 및 IP 회선 유닛 개별증명서와 함께 OK 메시지를 VTE(81)에 송신한다

(S219). VTE(81)는, OK 메시지를 수신하면, IP 회선 유닛 IP 어드레스 및 IP 회선 유닛 개별증명서를 기억부(125)에 유지하고, ACK 메시지를 SIP 서버(37)에 회신하고(S221), 또한 이용자 PC(85)에 SIP 접속의 확립을 통지한다(S223). SIP 서버(37)는 ACK 메시지를 IP 회선 유닛(63)에 송신한다(S225).

[0104] 상기의 과정에서, IP 회선 유닛(63)과 VTE(81) 사이에서, IP 어드레스 및 전자증명서가 교환되고 있다. IP 회선 유닛(63)은, ACK 메시지를 수신하면, VPN 접속 요구를 VTE(81)에 대하여 행한다(S227). VPN 접속은 SIP 서버(37)를 통하지 않고 행해진다. VTE(81)는 상대편의 VTE-IP 어드레스를 포함하는 착신 정보를 이용자 PC(85)에 보낸다(S229). 또한 VTE(81)는 VPN 서버로서 VPN 접속의 처리를 행한 것을 IP 회선 유닛(63)에 통지한다(S231). IP 회선 유닛(63)은 상대편의 VTE-IP 어드레스를 포함하는 착신 정보를 컨트롤러(61)에 보낸다(S233). 이렇게 하여, VPN 접속이 확립되고, 단말 간 VPN(25)을 통하여 정보가 통신된다.

[0105] 도 6, 도 7에 도시되는 바와 같이, 양 도면의 처리에서, VPN 접속 요구는 IP 회선 유닛(63)으로부터 VTE(81)에 보내지고 있다. 이 이유는 이하와 같다. VPN에서는 접속 요구가 클라이언트로부터 서버에 보내질 필요가 있다. 본 실시형태에서는, VPN 서버의 기능이 VTE(81)에만 설치되어 있다. 그 때문에 도 6 및 도 7의 쌍방에 있어서, VPN 접속 요구가 IP 회선 유닛(63)으로부터 VTE(81)로 보내진다.

[0106] 이상으로 본 발명의 적합한 실시형태에 대하여 설명했다. 본 실시형태에 의하면, 복수의 단말(감시 장치(15), 이용자 장치(17))이 SIP 서버(37)를 구비한 통신 관리 장치(11)와 접속된다. 도 3에 도시한 바와 같이, 통신 관리 장치(11)는, SIP 서버(37)에 더하여, 인가 정보 기억부(101)와 인가 처리부(103)를 갖는다. SIP의 시그널링에서는, INVITE(초대) 메시지가 접속원의 단말로부터 SIP 서버에 보내진다. 이 때, 인가 처리부(103)가 접속을 인가할지 아닐지를 판정한다. 인가 처리부(103)가 접속을 인가한 경우만, SIP 서버(37)가 접속원의 단말로부터의 INVITE 메시지를 접속처의 단말에 보내고, SIP의 시그널링이 성공한다.

[0107] 이와 같이, 본 발명에서는, 접속이 인가될 단말의 조합의 정보를 미리 기억해 두고, SIP의 시그널링 시에 단말 간의 접속의 인가를 행한다. 이것에 의해, 단말과 SIP 서버(37) 간의 단순한 인증이 아니고, SIP 서버(37)를 통한 단말 간 즉 P2P에 대한 인가를 행할 수 있어, 감시 정보의 이용자를 적합하게 제한할 수 있다. 이렇게 하여, 감시 시스템(1)에 SIP를 적용하는 경우의 세큐러티성을 향상할 수 있다.

[0108] 또한, 본 발명에서는, SIP의 시그널링에 있어서의 INVITE 메시지와 OK 메시지의 교환에, 통신 관리 장치(11)를 통하지 않는 단말 간 접속의 확립에 사용하는 접속 확립 정보가 부가될 수도 있다. 이것에 의해, 접속 확립 정보가 단말 간에 교환되어, 단말 간 접속을 확립할 수 있다. 이와 같이 하여, SIP를 능숙하게 이용하여, 단말 간 접속을 행할 수 있다. 그리고, 통신 관리 장치(11)와 단말의 통신량을 저감하여, 통신 관리 장치(11)의 부하를 경감할 수 있다.

[0109] 또한, 본 실시형태에서는, 접속 확립 정보로서 IP 어드레스와 전자증명서를 예로 들어 설명했지만, 전자증명서 대신에 다른 정보를 사용하여 상대방의 인증을 행하도록 해도 된다. 예를 들면, 전자증명서에 포함되는 커먼 네임 등을 접속 확립 정보로서 사용해도 된다.

[0110] 또한, 본 발명에 의하면, 통신 관리 장치(11)를 통하지 않는 단말 간 접속이 단말 간에 VPN을 구축하여 접속하는 단말 간 VPN(25)일 수도 있다. SIP의 시그널링에 있어서의 쌍방향의 메시지 교환을 VPN 접속 확립에 필요한 정보의 교환에 적합하게 이용할 수 있고, 그리고, VPN의 적용에 의해 세큐러티성을 높게 할 수 있다.

[0111] 또한 본 발명에 의하면, 초대 메시지가 접속원의 단말의 IP 어드레스와 전자증명서를 접속 확립 정보로서 포함하고, OK 메시지가 접속처의 단말의 IP 어드레스와 전자증명서를 접속 확립 정보로서 포함할 수도 있다. 이것에 의해, SIP를 적합하게 이용하여, VPN 접속에 사용하는 정보를 교환하고, 단말 간에 안전한 통신을 행할 수 있다.

[0112] 또한 본 발명에 의하면, 통신 관리 장치(11)가 감시 센터(3)에 설치될 수도 있다. 이것에 의해, 통신 관리 장치(11)를 이용하여, 감시 센터(3)와 단말의 통신 및 단말 간의 통신을 적합하게 행할 수 있다.

[0113] 또, 본 발명에 의하면, 통신 관리 장치(11)와 복수의 단말과의 접속은 통신 관리 장치(11)와 복수의 단말 사이에 VPN을 구축한 센터 단말 간 VPN(21)에 의해 접속될 수도 있고, SIP 서버(37)는 센터 단말 간 VPN(21)을 통하여 복수의 단말과 SIP 메시지를 통신할 수도 있다. 이것에 의해 SIP 통신이 센터 단말 간 VPN(21)상에서 행해진다. SIP 세션 후에 확립되는 단말 간 VPN(25)이 단말 간의 VPN인 것에 대하여, 센터 단말 간 VPN(21)은 통신 관리 장치(11)와 단말 간의 VPN이다. 센터 단말 간 VPN(21)을 사용함으로써, 감시 센터(3)와 각 단말의 통신의 세큐러티를 확보할 수 있고, 그리고, SIP 통신의 세큐러티도 확보할 수 있다.

[0114] 또한 본 발명에 의하면, 감시 정보가 감시대상(5)에서 촬영된 화상, 감시대상(5)에서 검출된 감시 신호, 이용자 측에서 생성된 제어 정보 중 적어도 하나를 포함할 수도 있다. 이것에 의해, 단말 간에 유용한 감시 정보를 통신할 수 있다.

[0115] 이상으로 본 발명의 적합한 실시형태를 설명했다. 그러나, 본 발명은 상기의 실시형태에 한정되지 않고, 당업자가 본 발명의 범위 내에서 상기의 실시형태를 변형가능한 것은 물론이다.

[0116] 이상으로 현시점에서 생각할 수 있는 본 발명의 적합한 실시형태를 설명했는데, 본 실시형태에 대하여 다양한 변형이 가능한 것이 이해되며, 그리고, 본 발명의 진실한 정신과 범위 내에 있는 그와 같은 모든 변형을 첨부의 청구범위가 포함하는 것이 의도되어 있다.

[0117] (산업상의 이용가능성)

[0118] 이상과 같이, 본 발명에 따른 감시 시스템은 통신을 사용하여 원격지에서 점포 등을 감시하기 위하여 유용하다.

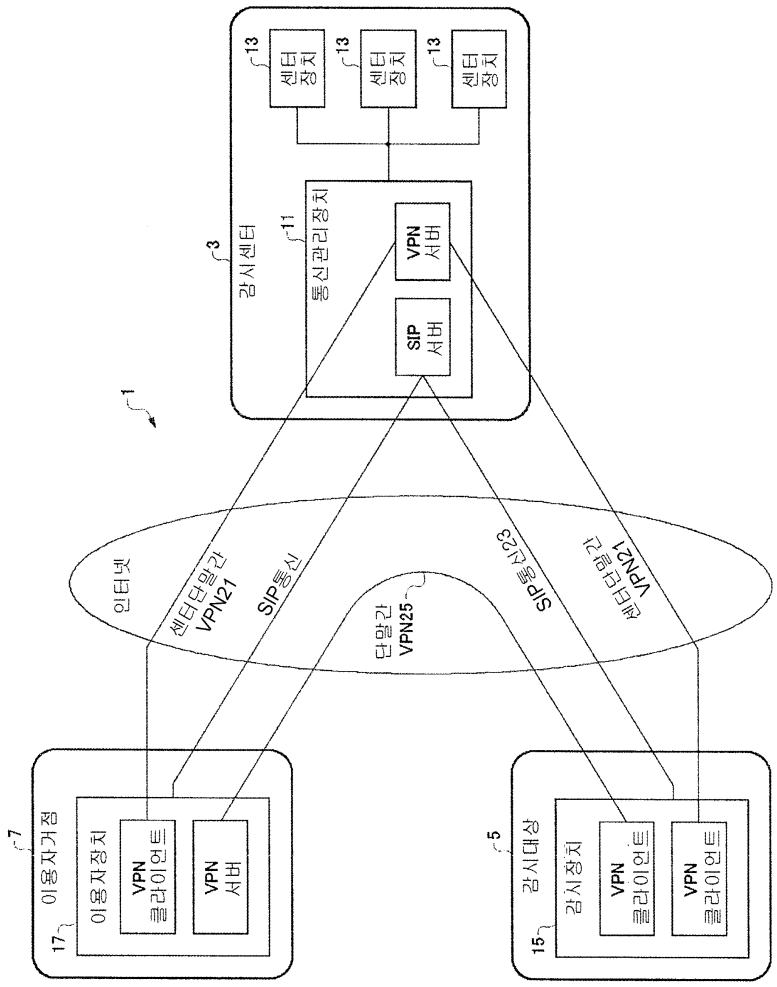
부호의 설명

[0119]

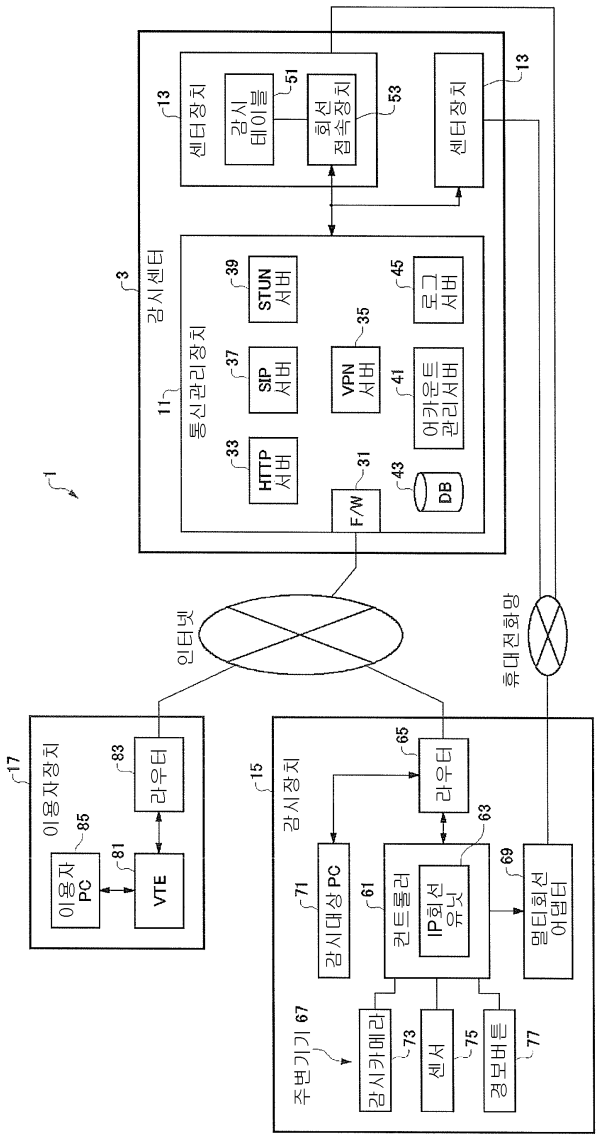
1 감시 시스템	3 감시 센터
5 감시대상	7 이용자 거점
11 통신 관리 장치	13 센터 장치
15 감시 장치	17 이용자 장치
21 센터 단말 간 VPN	23 SIP 통신
25 단말 간 VPN	33 HTTP 서버
35 VPN 서버	37 SIP 서버
41 어카운트 관리 서버	43 데이터 베이스
61 컨트롤러	63 IP 회선 유닛
65, 83 라우터	69 멀티 회선 어댑터
73 감시 카메라	81 VPN 종단 장치(VTE)
85 이용자 PC	101 인가 정보 기억부
103 인가 처리부	

도면

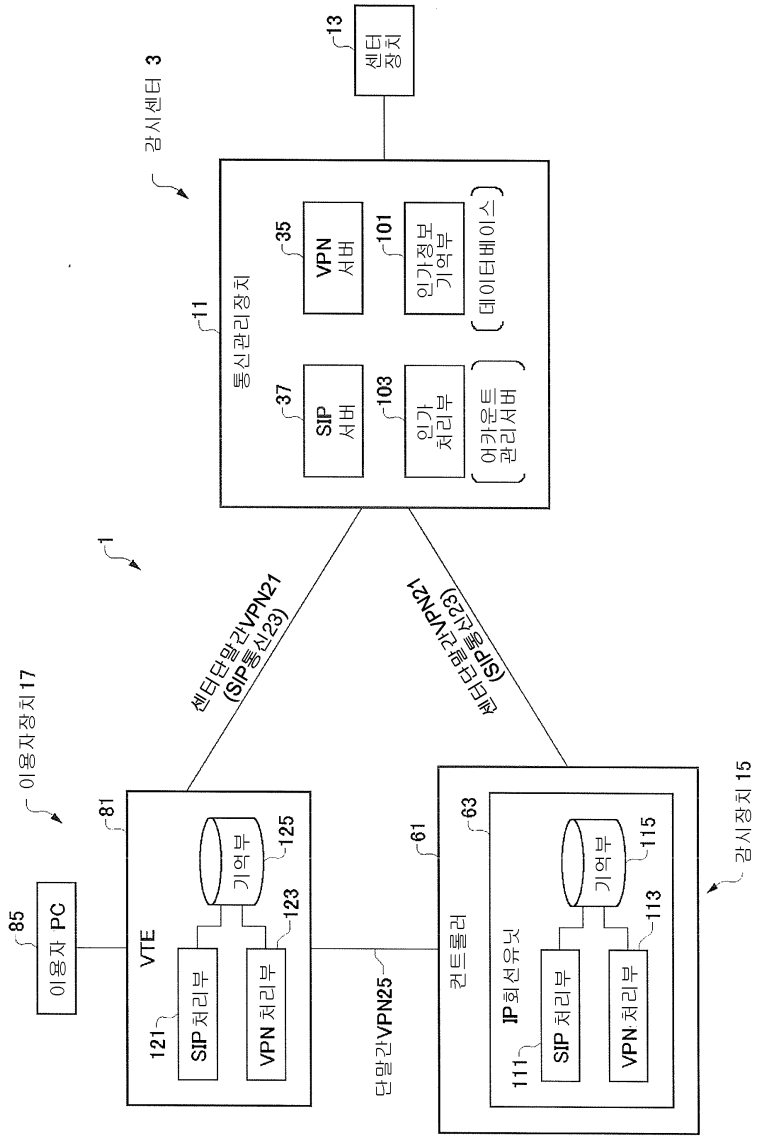
도면1


1
3
감시센터
11
통신관리장치
VPN
서버
SIP
서버
13
센터
장치
13
센터
장치
13
센터
장치
인터넷
센터단말간
VPN21
SIP통신
단말간
VPN25
SIP신호23
긴급데이터망
VPN21
7
이용자거점
17
이용자장치
VPN
클라이언트
VPN
서버
5
감시대상
15
감시장치
VPN
클라이언트
VPN
클라이언트

도면2


1
3 감시센터
11 통신관리장치
33 HTTP 서버
37 SIP 서버
39 STUN 서버
35 VPN 서버
41 어카운트 관리서버
45 로그 서버
31 F/W
43 DB
13 센터장치
51 감시 테이블
53 회선 접속장치
13 센터장치
인터넷
휴대전화망
17 이용자장치
85 이용자 PC
81 VTE
83 라우터
15 감시장치
71 감시대상 PC
61 컨트롤러
IP회선 유닛
63
65 라우터
69 멀티회선 어댑터
주변기기 67
73 감시카메라
75 센서
77 경보버튼

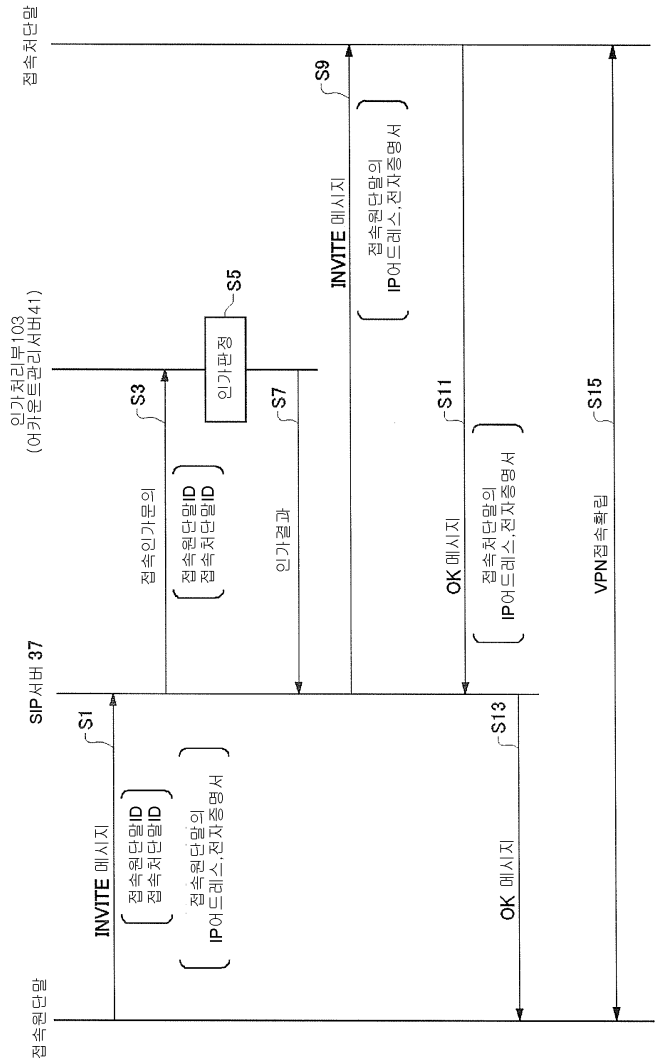
도면3


감시센터 3
13
센터 장치
11
통신관리장치
35
VPN 서버
101
인가정보 기억부
데이터베이스
37
SIP 서버
103
인가 처리부
어카운트 관리서버
1
센터단말간VPN21 (SIP통신23)
(SIP통신23)센터단말간VPN21
이용자장치17
85
이용자 PC
81
VTE
121
SIP 처리부
123
VPN 처리부
125
기억부
단말간VPN25
61
컨트롤러
63
IP회선유닛
111
SIP 처리부
113
VPN 처리부
115
기억부
감시장치 15

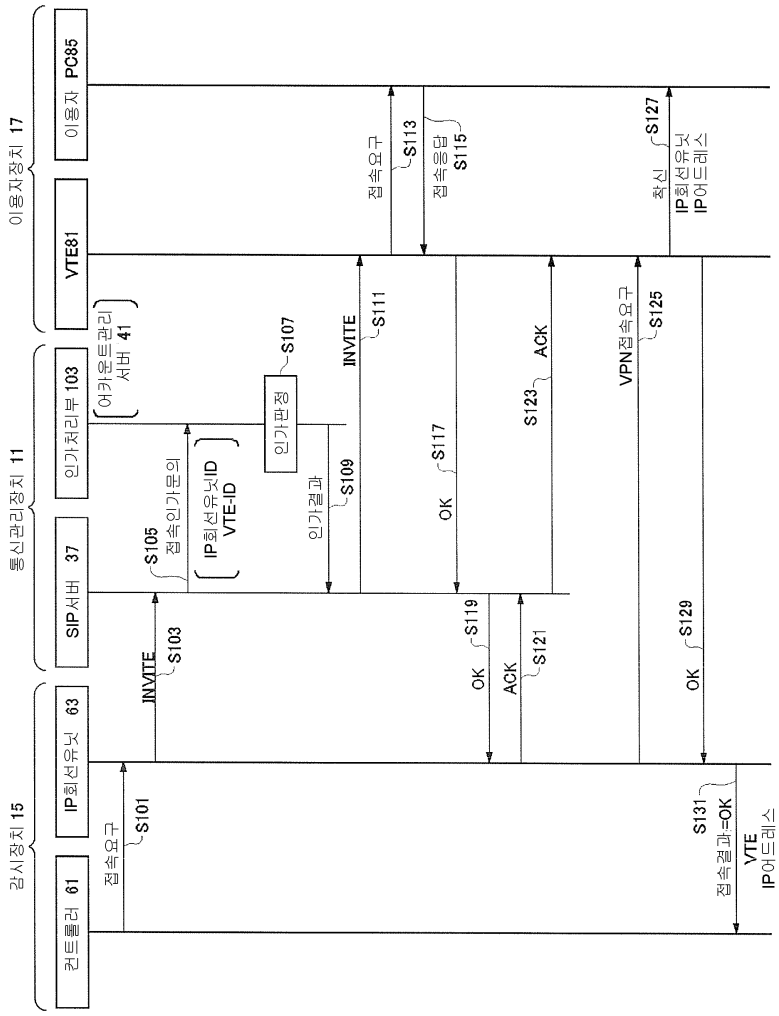
도면4

이용자 (오너)	단말ID	
	감시장치ID	이용자장치ID
A	A01	A11
B	B01	B11
C	C01	C11
C	C02	C11
...	...	...

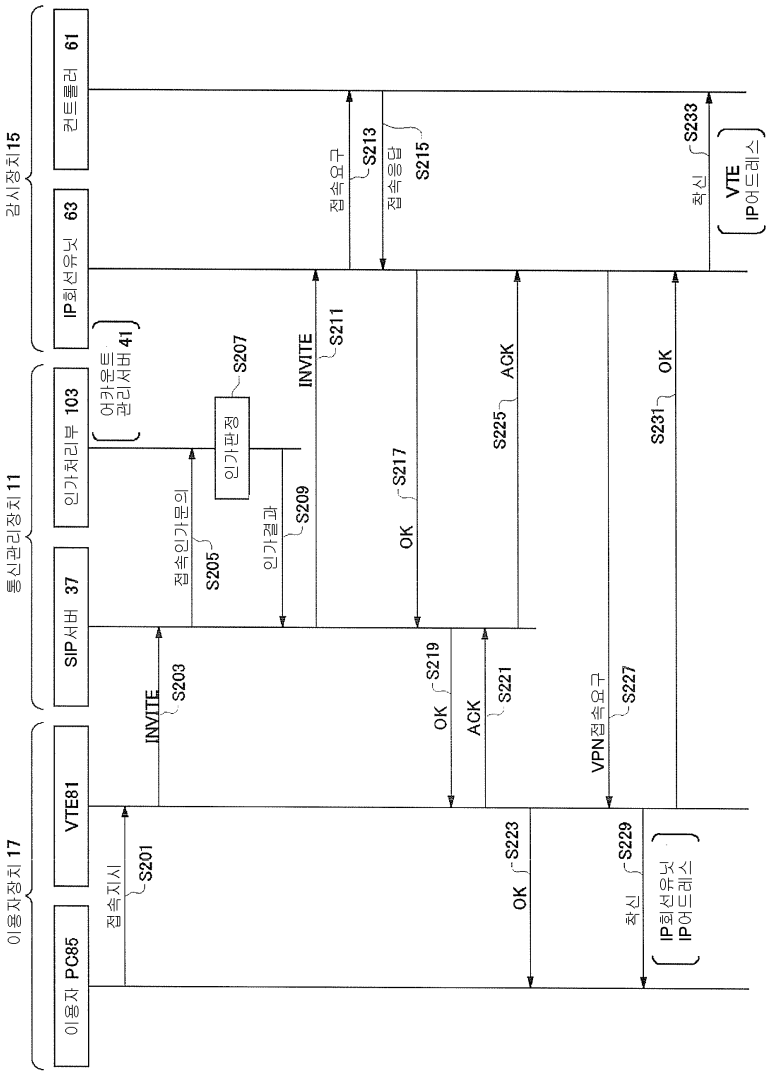
도면5



도면6


감시장치 15
통신관리장치 11
이용자장치 17
컨트롤러 61
IP회선유닛 63
SIP서버 37
인가처리부 103
어카운트관리 서버 41
VTE81
이용자 PC85
접속요구
S101
INVITE
S103
접속인가문의
IP회선유닛ID
VTE-ID
S105
인가결과
S109
인가판정
S107
INVITE
S111
접속요구
S113
접속응답
S115
OK
S117
OK
S119
ACK
S121
ACK
S123
VPN접속요구
S125
OK
S129
확신
IP회선유닛
IP어드레스
S127
S131
접속결과=OK
VTE
IP어드레스

도면7


이용자장치 17
이용자 PC85
VTE81
통신관리장치 11
SIP서버 37
인가처리부 103
어카운트 관리서버 41
감시장치 15
IP회선유닛 63
컨트롤러 61
접속지시
S201
INVITE
S203
접속인가문의
S205
인가판정
S207
인가결과
S209
INVITE
S211
접속요구
S213
접속응답
S215
착신
S233
VTE
IP어드레스
OK
S217
ACK
S225
OK
S231
OK
S219
ACK
S221
VPN접속요구
S227
OK
S223
착신
S229
IP회선유닛
IP어드레스