(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년05월16일
(11) 등록번호 10-1858207
(24) 등록일자 2018년05월09일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/62* (2013.01)
(52) CPC특허분류
H04L 63/0272 (2013.01)
G06F 21/62 (2013.01)
(21) 출원번호 10-2017-0173081
(22) 출원일자 2017년12월15일
심사청구일자 2017년12월15일
(56) 선행기술조사문헌
KR1020140055562 A*
KR1020160000013 A*
KR1020080053824 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국병영정보문화원 주식회사
서울특별시 도봉구 도봉로137길 16 (쌍문동)
(72) 발명자
나주희
서울특별시 성북구 아리랑로 75, 102동 304호 (돈암동, 돈암코오롱하늘채)
(74) 대리인
특허법인메이저

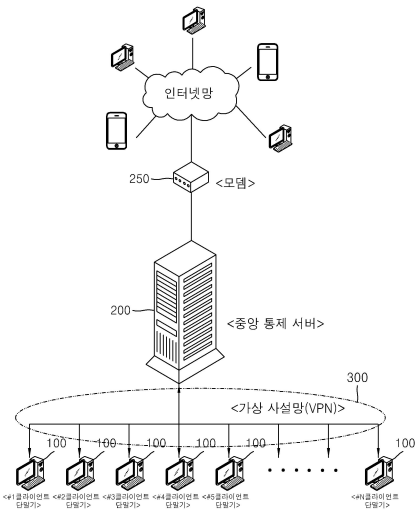
전체 청구항 수 : 총 8 항 심사관 : 문형섭

(54) 발명의 명칭 **국군 여가복지전용 보안망 시스템**

(57) 요 약

본 발명의 실시 형태는 승인된 단말기 및 IP만 네트워크망을 이용하도록 하는 가상 사설망; 사용자가 사용하는 IP 할당된 단말기로서, 상기 가상 사설망을 통하여 인터넷 접속을 요청하는 클라이언트 단말기; 및 상기 가상 사설망에 접속한 클라이언트 단말기들 중에서, 승인된 단말기 및 IP만 인터넷에 접속되도록 하며, 비승인된 단말기 및 IP는 인터넷 접속을 원천차단하는 중앙 통제 서버;를 포함하며, 상기 클라이언트 단말기는, 인증된 사용자만 단말기의 운영 시스템(OS)을 이용할 수 있도록 하는 시스템 보안 모듈; 및 문자 채팅 프로그램, 보이스 채팅 프로그램, 및 온라인 게임 프로그램을 포함하는 비승인 프로그램의 동작을 차단하는 프로그램 보안 모듈;이 설치되어 있을 수 있다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/0236 (2013.01)
H04L 63/102 (2013.01)

명 세 서

청구범위

청구항 1

승인된 단말기 및 IP만 네트워크망을 이용하도록 하는 가상 사설망;

사용자가 사용하는 IP 할당된 단말기로서, 상기 가상 사설망을 통하여 인터넷 접속을 요청하는 클라이언트 단말기; 및

상기 가상 사설망에 접속한 클라이언트 단말기들 중에서, 승인된 단말기 및 IP만 인터넷에 접속되도록 하며, 비승인된 단말기 및 IP는 인터넷 접속을 원천차단하는 중앙 통제 서버;를 포함하며,

상기 클라이언트 단말기는,

인증된 사용자만 단말기의 운영 시스템(OS)을 이용할 수 있도록 하는 시스템 보안 모듈; 및

문자 채팅 프로그램, 보이스 채팅 프로그램, 및 온라인 게임 프로그램을 포함하는 비승인 프로그램의 동작을 차단하는 프로그램 보안 모듈;을 포함하고,

상기 프로그램 보안 모듈은,

로그인한 사용자의 사용자 군대계급, 사용자 군번, 사용자 소속 부대를 포함하는 사용자 정보를 암호화한 보안 코드를 생성하며 데이터베이스에 저장하며, 사용자에 의해 작성되는 문서 파일에 상기 보안 코드를 함께 포함시키고,

상기 프로그램 보안 모듈은,

상기 데이터베이스에 저장된 보안 코드를 제1보안 코드와 제2보안 코드로서 분할하여 상기 제1보안 코드만 사용자에 의해 작성되는 문서 파일에 함께 포함하고, 상기 제2보안 코드는 사용자의 상급 장교의 로그인 정보에 포함시켜 저장하며,

상기 사용자에 의해 작성되는 문서 파일이 호출될 때 문서 파일에 포함된 제1보안 코드를 추출하고, 상기 사용자의 상급 장교로부터 로그인 승인이 있는 경우에 한하여 상기 제2보안 코드를 추출하여, 추출한 제1보안 코드와 제2보안 코드를 결합하여 보안 코드를 생성하며, 결합 생성한 보안 코드와 프로그램 보안 모듈의 데이터베이스에 있는 보안 코드가 서로 일치하는 경우에만 문서 파일이 표시되도록 하는 국군 여가복지전용 보안망 시스템.

청구항 2

청구항 1에 있어서, 상기 시스템 보안 모듈은,

로그인한 사용자의 보안 등급에 따라서 윈도우 폴더의 접근 권한을 제한함을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 3

청구항 1에 있어서, 상기 시스템 보안 모듈은,

로그인한 사용자의 보안 등급에 따라서 시스템 파일(DOS/config)의 접근 권한을 제한함을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 4

청구항 1에 있어서, 상기 시스템 보안 모듈은,

백업 프로그램을 구동시킴을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 5

청구항 1에 있어서, 상기 프로그램 보안 모듈은,

사용자 개인정보, 포인트 정보, 사용자 로그인 이력 정보를 포함하는 사용자 정보를 암호화하여 저장함을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 6

청구항 1에 있어서, 상기 프로그램 보안 모듈은,

원격 제어에 의한 구동이 이루어짐을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 7

청구항 1에 있어서, 상기 프로그램 보안 모듈은,

사이트에서 이루어지는 결제를 차단함을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 8

청구항 1에 있어서, 상기 중앙 통제 서버는,

사용이 허가된 프로그램 리스트와 프로그램별로 이용 가능한 계급 정보인 승인 계급 정보를 상기 클라이언트 단말기로 전송하며,

상기 프로그램 보안 모듈은, 사용자가 접근하려는 프로그램에 할당된 승인 계급 정보와 로그인한 사용자의 계급 정보가 일치하는 경우에만 프로그램 구동이 되도록 함을 특징으로 하는 국군 여가복지전용 보안망 시스템.

청구항 9

삭제

청구항 10

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 보안망 시스템으로서, 군사보안 환경에 맞는 국군 여가복지전용 보안망 시스템에 관한 것이다.

배 경 기 술

[0003] 정보유출의 대부분의 경로는 조직의 외부자가 아닌 내부자의 소행이라는 통계가 있다. 인터넷망을 통한 외부 해커 침입보다는 조직내의 소속 구성원들이 스파이처럼 네트워크를 통해 온라인으로 정보를 유출하는 경우가 많다.

[0004] 예를 들어, 2016년 09월의 외부망과 내부망 관리 부재로 인한 국방망 해킹 보안사고, 병영 내 사이버지식정보방

보안사고, 장병 사행성 도박 및 음란성 사이트 접속 사고 등이 발생하고 있다.

[0005] 따라서 국방 기관들은 정보유출 방지에 많은 관심을 가지고 있고 그 일환으로 네트워크를 통한 정보유출만이라도 막기위해 프록시(방화벽)을 설치하여 외부의 해커 및 내부 구성원의 네트워크를 통한 정보 누수를 막고 있다.

[0006] 이와 같이, 내부 인트라넷만을 사용하는 환경은 정보유출을 우려해 외부로 나갈 수 있는 통로 자체를 제거함으로서 그 정보를 보호해 왔다. 즉, 도 1에서와 같이 정보 보호를 위해 외부 연결을 이어주는 서버와의 연결 자체를 제거함으로써 그 정보를 보호하려 시도하였다.

[0007] 예를 들어, 일반적인 군부대의 PC실에서 내부적 인트라넷만을 구성하여 군 대원들을 교육하지만 외부와의 연결을 통한 실질적인 인터넷을 사용하지는 못하게 되어 있다. 또한 정보를 기반으로 하는 산업의 업체에서도 중요한 내부 업무 관련 정보를 다른 서버에 사용함 으로써 외부와의 연결을 분리하여 하여 사용하고 있다.

[0008] 외부인터넷과 연결이 차단된 내부 인트라넷만을 사용하는 과정을 살펴보면, 먼저 도 1의 일반 사용자들이 PC를 사용하면 PC의 데이터나 통신내용이 관리하는 서버로 그 데이터를 전송하게 된다. 인터넷 환경으로 연결되는 경로 자체가 차단되어 있어 외부적인 정보 유출 자체를 차단할 수 있다.

[0009] 그러나 사용자들 PC와 서버가 구축되어 있는 환경에서 외부 인터넷을 연결하지 않고 사용하지 못하는 것은 정보보호를 위해서는 최선이지만 자원을 낭비하는 결과를 가져오게 되는 것이다.

[0010] 특히, 군사보안 환경에 맞지 않는 시스템 활용으로 현재까지 보안과 관련되어 사회와 동일한 콘텐츠를 병영 내에서 사용 불가하게 되는 문제가 있다. 이는 장병들의 문화적 이질감 및 복무의욕 저하 등 시대에 맞지 않는 복지 제공으로 문화 낙후가 지속되고 있다.

[0011] 이러한 문제점을 해결하고자 군사보안 환경에 맞는 화이트리스트 개념의 복지전용 보안망 시스템의 개발 필요성이 절실하다.

선행기술문헌

특허문헌

[0013] (특허문헌 0001) 한국공개특허 10-2001-0078840

발명의 내용

해결하려는 과제

[0014] 본 발명의 기술적 과제는 군사보안 환경에 맞는 국군 여가복지전용 보안망을 제공하는데 있다.

과제의 해결 수단

[0016] 본 발명의 실시 형태는 승인된 단말기 및 IP만 네트워크망을 이용하도록 하는 가상 사설망; 사용자가 사용하는 IP 할당된 단말기로서, 상기 가상 사설망을 통하여 인터넷 접속을 요청하는 클라이언트 단말기; 및 상기 가상 사설망에 접속한 클라이언트 단말기들 중에서, 승인된 단말기 및 IP만 인터넷에 접속되도록 하며, 비승인된 단말기 및 IP는 인터넷 접속을 원천차단하는 중앙 통제 서버;를 포함하며, 상기 클라이언트 단말기는, 인증된 사용자만 단말기의 운영 시스템(OS)을 이용할 수 있도록 하는 시스템 보안 모듈; 및 문자 채팅 프로그램, 보이스 채팅 프로그램, 및 온라인 게임 프로그램을 포함하는 비승인 프로그램의 동작을 차단하는 프로그램 보안 모듈;을 포함하고, 상기 프로그램 보안 모듈은, 로그인한 사용자의 사용자 군대계급, 사용자 군번, 사용자 소속 부대를 포함하는 사용자 정보를 암호화한 보안 코드를 생성하며 데이터베이스에 저장하며, 사용자에 의해 작성되는 문서 파일에 상기 보안 코드를 함께 포함시키고, 상기 프로그램 보안 모듈은, 상기 데이터베이스에 저장된 보안 코드를 제1보안 코드와 제2보안 코드로서 분할하여 상기 제1보안 코드만 사용자에 의해 작성되는 문서 파일에 함께 포함하고, 상기 제2보안 코드는 사용자의 상급 장교의 로그인 정보에 포함시켜 저장하며, 상기 사용자에 의해 작성되는 문서 파일이 호출될 때 문서 파일에 포함된 제1보안 코드를 추출하고, 상기 사용자의 상급 장교로부터 로그인 승인이 있는 경우에 한하여 상기 제2보안 코드를 추출하여, 추출한 제1보안 코드와 제2보안 코드를 결합하여 보안 코드를 생성하며, 결합 생성한 보안 코드와 프로그램 보안 모듈의 데이터베이스에 있는 보안

코드가 서로 일치하는 경우에만 문서 파일이 표시하는 것을 특징으로 한다.

[0017] 상기 시스템 보안 모듈은, 로그인한 사용자의 보안 등급에 따라서 윈도우 폴더의 접근 권한을 제한할 수 있다.

[0018] 상기 시스템 보안 모듈은, 로그인한 사용자의 보안 등급에 따라서 시스템 파일(DOS/config)의 접근 권한을 제한할 수 있다.

[0019] 상기 시스템 보안 모듈은, 백업 프로그램을 구동시킴을 특징으로 할 수 있다.

[0020] 상기 프로그램 보안 모듈은, 사용자 개인정보, 포인트 정보, 사용자 로그인 이력 정보를 포함하는 사용자 정보를 암호화하여 저장함을 특징으로 할 수 있다.

[0021] 상기 프로그램 보안 모듈은, 원격 제어에 의한 구동이 이루어짐을 특징으로 할 수 있다.

[0022] 상기 프로그램 보안 모듈은, 사이트에서 이루어지는 결제를 차단할 수 있다.

[0023] 상기 중앙 통제 서버는, 사용이 허가된 프로그램 리스트와 프로그램별로 이용 가능한 계급 정보인 승인 계급 정보를 상기 클라이언트 단말기로 전송하며, 상기 프로그램 보안 모듈은, 사용자가 접근하려는 프로그램에 할당된 승인 계급 정보와 로그인한 사용자의 계급 정보가 일치하는 경우에만 프로그램 구동이 되도록 할 수 있다.

[0024] 삭제

[0025] 삭제

발명의 효과

[0027] 본 발명의 실시 형태에 따르면 클라이언트 단말기 측에서 프로그램 보안 동작과 시스템 보안 동작을 수행함으로써, 방화벽을 통한 물리적 차단없이도 보안성이 향상된 국군 여가복지 네트워크를 제공해줄 수 있게 된다.

도면의 간단한 설명

[0029] 도 1은 기존의 방화벽이 설치된 보안망 시스템 구성도.

도 2는 본 발명의 실시예에 따른 국군 여가복지전용 보안망 시스템의 구성도.

도 3은 본 발명의 실시예에 따른 국군 여가복지전용 보안망 시스템의 동작 설명을 도시한 그림.

도 4는 본 발명의 실시예에 따른 클라이언트 단말기의 구성 블록도.

도 5는 본 발명의 실시예에 따른 문서 파일의 보안 코드의 저장 예시 그림.

도 6은 본 발명의 실시예에 따른 사용자의 상급 장교로부터 문서 파일 인증을 받는 인증창.

발명을 실시하기 위한 구체적인 내용

[0030] 이하, 본 발명의 장점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은, 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것으로, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 또한, 본 발명을 설명함에 있어 관련된 공지 기술 등이 본 발명의 요지를 흐리게 할 수 있다고 판단되는 경우 그에 관한 자세한 설명은 생략하기로 한다.

[0031] 도 2는 본 발명의 실시예에 따른 국군 여가복지전용 보안망 시스템의 구성도이며, 도 3은 본 발명의 실시예에 따른 국군 여가복지전용 보안망 시스템의 동작 설명을 도시한 그림이며, 도 4는 본 발명의 실시예에 따른 클라이언트 단말기의 구성 블록도이다.

[0032] 본 발명의 국군 여가복지전용 보안망 시스템은, 도 2 및 도 3에 도시한 바와 같이 가상 사설망(300), 클라이언트 단말기(100), 및 중앙 통제 서버(200)를 포함할 수 있다. 이밖에 모뎀(250)을 더 포함할 수 있다.

[0033] 가상 사설망(300)은, 승인된 단말기 및 IP만 네트워크망을 이용할 수 있도록 하는 네트워크망이다. 따라서 내부

망 체계로서 외부 사설 IP 접속이 불가능하다.

[0034] 알려진 바와 같이, 가상 사설망(300)(VPN;Virtual Private Network)은, 인터넷과 같은 공중망(public network)을 마치 전용선으로 사설망(private network)을 구축한 것처럼 사용할 수 있는 방식의 네트워크망을 말한다. 네트워크망의 고비용과 비효율적인 관리를 해결하기 위한 방법으로 인터넷망을 마치 전용선으로 사설망을 구축한 것처럼 사용하는 방식이 대두하게 되었는데 이를 가상사설망이라 한다. 가상사설망은 기업의 통신망과 인터넷 서비스 제공자와 연결만 하면 되기 때문에 별도로 값비싼 장비나 소프트웨어를 구입하고 관리할 필요가 없어 기존의 사설망 연결방식보다 비용이 대폭 절감되는 장점을 가진다.

[0035] 하지만, 가상 사설망(300)은 인터넷이라는 공중망을 기본으로 하기 때문에 적절한 통신속도 및 대역폭의 보장과, 무엇보다 정보에 대한 보안이 확실하지 않다는 점이 큰 단점을 가진다. 이에 본 발명은, 승인된 단말기 및 IP만 네트워크망을 이용하도록 한다. 즉, 휴대폰이나 단말기별로 고유의 하드웨어 식별번호인 MAC, IMEI를 가지고 있는데 승인된 MAC, IMEI를 가지는 단말기만이 가상 사설망(300)을 이용하도록 하는 것이다. 마찬가지로 네트워크에 연결되는 단말기별로 IP 주소(IP address)가 할당되는데, 허가된 IP 주소를 통해 접속시에만 가상 사설망(300)을 이용 가능하도록 한다.

[0037] 중앙 통제 서버(200)는, 모뎀(250)을 통하여 통신회선 보안을 유지할 수 있다. 즉, 인터넷 수신 단말기인 모뎀(250)과 중앙통제서버(200)간에 상호 암호화된 인증값을 공유하여 인증값의 신호가 바뀌거나 끊길 경우 인터넷 신호를 자동 차단 등을 통해 방어할 수 있게 된다.

[0038] 중앙 통제 서버(200)는 가상 사설망(300)에 접속한 클라이언트 단말기(100)들 중에서, 승인된 단말기 및 IP(화이트 리스트)만 인터넷에 접속되도록 하며, 비승인된 단말기 및 IP(블랙 리스트)는 인터넷 접속을 원천차단한다. 가상 사설망(300)에서 1차적으로 인터넷 접속 여부를 결정하지만, 추가적으로 중앙통제서버에서 2차적으로 승인된 사용자만 인터넷 접속이 가능하도록 결정한다. 따라서 비승인된 단말기 및 IP 접속 시에는 인터넷을 원천 차단한다. 비승인 접속하는 이벤트 발생시에는 관리자에게 알람 경고한다.

[0039] 이를 위하여 중앙 통제 서버(200)는, 하드웨어적으로는 통상적인 웹 서버와 동일한 구성을 가지며, 소프트웨어적으로는 C, C++, Java, Visual Basic, Visual C 등과 같은 다양한 형태의 언어를 통해 구현되어 여러 가지 기능을 하는 프로그램 모듈을 포함한다. 또한, 일반적인 서버용 하드웨어에 도스(dos), 윈도우(window), 리눅스(linux), 유닉스(unix), 매킨토시(macintosh) 등의 운영 체제에 따라 다양하게 제공되고 있는 웹 서버 프로그램을 이용하여 구현될 수 있으며, 대표적인 것으로는 윈도우 환경에서 사용되는 웹사이트(website), IIS(Internet Information Server)와 유닉스 환경에서 사용되는 CERN, NCSA, APPACH 등이 이용될 수 있다.

[0040] 중앙 통제 서버(200)와 클라이언트 단말기(100)는 보안 세션에 관여한다. SSL 또는 TLS 세션은 핸드세이크 프로토콜(a handshake protocol)에 의해 생성되는 클라이언트와 서버 사이의 연관(an association)이다. 세션은 암호 보안 파라미터의 세트를 규정하는데, 이는 다수의 접속들 사이에서 공유될 수 있다. 그들은 개개의 접속에 대한 신규의 보안 파라미터의 고가의 협상(negotiation)을 피하기 위해 사용된다. SSL 또는 TLS에서, 세션 식별자(session identifier)는 특정 세션을 식별하는 서버에 의해 생성된 값이다. SSL 또는 TLS 세션을 확립하기 위해, 클라이언트 및 서버는 핸드셰이크를 수행하는데, 이는 개체들 사이의 트랜잭션의 파라미터(parameters of transaction)를 확립하는 최초의 협상이다. 세션이 생성되면, 중앙 통제 서버(200)와 클라이언트 단말기(100) 사이의 통신은 접속을 통해 발생하는데, 이는 (OSI 계층 모델 정의에) 적합한 유형의 서비스를 제공하는 전송이다. SSL 및 TLS의 경우, 그러한 접속은 피어 투 피어 관계(peer-to-peer relationship)이다. 접속은 일시적이고 모든 접속은 하나의 세션과 연관된다. 전형적으로, 접속을 통한 통신은 공개 키 암호(public key cryptography)를 사용하여 보호되는데, 이는 2 키 암호(two-key ciphers)를 이용하는 암호화 기술의 일종이다. 공개 키로 암호화된 메시지는 연관된 특정 키로만 암호해독될 수 있다. 반대로, 특정 키로 서명된 메시지는 공개 키를 이용하여 인증될 수 있다. 일단 세션이 확립되면, 클라이언트 단말기(100)는 인증서를 갖는데, 이러한 인증서는 클라이언트 단말기(100)를 중앙 통제 서버(200)에 인증시키기 위해 중앙 통제 서버(200)에 의해 발행된다. 클라이언트 단말기(100)도 중앙 통제 서버(200)를 유효한 것으로서 인증하기 위해 중앙 통제 서버(200)에 인증서를 제시하도록 요청할 수 있다. 인증(authentication)이란 하나의 개체가 또 다른 개체의 식별을 결정하는 능력이다. 전형적으로, X.509 프로토콜(별칭으로서 ISO 인증 프레임워크)의 일부로서, 인증서는 신뢰된 인증 권한에 의해 부여되고 사용자의 신원(party's identity)(또는 몇몇 다른 속성)과 그 공개 키 사이에 강한 결속을 제공한다.

[0041] 이러한 중앙 통제 서버(200)와 클라이언트 단말기(100) 간의 보안 통로는, 기능은 본 기술 분야에 잘 알려져 있다. 예를 들어, 기능은 IETF TLS 버전 1.0 및 SSL 버전 2.0/3.0에 승인된 프로토콜 내에서 구현된다. 이들 프로

토콜은 매우 단순하지만, 두 개의 층으로 이루어지는데, 기록 프로토콜(record protocol) 및 핸드셰이크 프로토콜(handshake protocol)이다.

[0043] 클라이언트 단말기(100)는 사용자가 사용하는 IP 할당된 단말기로서, 상기 가상 사설망(300)을 통하여 인터넷 접속을 요청한다. 여기서 클라이언트 단말기(100)는, 데스크탑 PC(desktop PC), 태블릿 PC(tablet PC), 슬레이트 PC(slate PC), 노트북 컴퓨터(notebook computer)등이 해당될 수 있다. 물론, 본 발명이 적용 가능한 단말기는 상술한 종류에 한정되지 않고, 외부 장치와 통신이 가능한 단말기를 모두 포함할 수 있음은 당연하다.

[0044] 클라이언트 단말기(100)는, 도 4에 도시한 바와 같이 시스템 보안 모듈(110)과 프로그램 보안 모듈(120)을 포함할 수 있다.

[0045] 시스템 보안 모듈(110)은, 인증된 사용자만 단말기의 운영 시스템(OS)을 이용할 수 있도록 한다.

[0046] 또한 시스템 보안 모듈(110)은, 로그인한 사용자의 보안 등급에 따라서 윈도우 폴더의 접근 권한을 제한한다. 클라이언트 단말기(100)에 로그인하는 사용자 정보로 보안등급을 확인하고 외부로 나갈 수 있는 정보의 등급을 결정짓는다. 사용자 정보의 보안 등급을 나눔으로서 사용할 수 있는 컨텐츠 즉 프로그램도 제한을 갖게 된다. 일반적인 메일에서 파일을 첨부하는 등에 제한을 가할 수 있다. 다시 말해 파일은 외부로 나갈 수 없다. 사용한 사용자의 시간과 접속한 경로 등을 체크해서 자료로 보관하며, 강제적인 작업을 진행하려 할 경우 프로그램을 닫아 버림으로서 사용자의 권한을 제거 시키는 기능을 수행한다.

[0047] 또한 시스템 보안 모듈(110)은, 로그인한 사용자의 보안 등급에 따라서 시스템 파일(DOS/config)의 접근 권한을 제한한다. 클라이언트 단말기(100)에 로그인하는 사용자 정보로 보안등급을 확인하고 시스템 파일의 접근 허가 여부를 결정한다.

[0048] 또한 시스템 보안 모듈(110)은, 백업 프로그램을 구동시켜, 시스템 관련 파일들을 백업 보관한다.

[0050] 프로그램 보안 모듈(120)은, 문자 채팅 프로그램, 보이스 채팅 프로그램, 및 온라인 게임 프로그램을 포함하는 비승인 프로그램의 동작을 차단하는 기능을 수행한다. 클라이언트 단말기(100)에 로그인한 사용자가 승인되지 않은 문자 채팅 프로그램, 보이스 채팅 프로그램, 및 온라인 게임 프로그램 등의 비승인 프로그램을 구동시키키려 하면, 해당 비승인 프로그램의 구동을 차단한다.

[0051] 또한 프로그램 보안 모듈(120)은, 사용자 개인정보, 포인트 정보, 사용자 로그인 이력 정보를 포함하는 사용자 정보를 암호화하여 저장한다. 예를 들어, 프로그램 보안 모듈(120)은, 각 사용자의 아이디를 가지고 있고, 사용자 아이디로 등록된 개인키/공개키 쌍이 존재한다. 또한 암호화를 위한 세션키 및 전자 서명을 위한 임시 개인키/공개키 쌍을 생성하고, 세션키로 암호화하거나 임시 개인키로 보안 설정값을 결정한다. 이러한 보안 설정값을 이용하여 사용자 정보를 암호화하여 저장한다. 암호화 저장되는 데이터베이스(DB;DataBase)는, 하드디스크 드라이브(Hard Disk Drive), SSD 드라이브(Solid State Drive), 플래시메모리(Flash Memory), CF카드(Compact Flash Card), SD카드(Secure Digital Card), SM카드(Smart Media Card), MMC 카드(Multi-Media Card) 또는 메모리 스틱(Memory Stick) 등 정보의 입출력이 가능한 모듈로서 장치의 내부에 구비되어 있을 수도 있고, 별도의 장치에 구비되어 있을 수도 있다.

[0052] 또한 프로그램 보안 모듈(120)은, 원격 제어에 의한 구동이 이루어지도록 한다.

[0053] 또한 프로그램 보안 모듈(120)은, 사이트에서 이루어지는 결제를 차단한다.

[0054] 또한 프로그램 보안 모듈(120)은, 사용자가 접근하려는 프로그램에 할당된 승인 계급 정보와 로그인한 사용자의 계급 정보가 일치하는 경우에만 프로그램 구동이 수행되도록 한다. 이를 위해 중앙 통제 서버(200)는, 사용이 허가된 프로그램 리스트와 프로그램별로 이용 가능한 계급 정보인 승인 계급 정보를 클라이언트 단말기(100)로 전송한다. 따라서 프로그램 보안 모듈(120)은, 각 프로그램별로 허가된 계급의 병사만 접근하도록 한다. 예를 들어, '워드 프로그램' 사용은 일병 계급 이상만 사용하도록 설정되어 있고, '파워포인트 프로그램' 사용은 병장 계급 이상만 사용하도록 설정되어 있다고 가정하면, 이등병 계급의 병사가 '파워포인트 프로그램'을 구동하더라도 '워드 프로그램'은 구동되지 않지만 '워드 프로그램'은 구동시킬 수 있게 된다.

[0056] 또한 프로그램 보안 모듈(120)은, 로그인한 사용자의 사용자 군대계급, 사용자 군번, 사용자 소속 부대를 포함하는 사용자 정보를 암호화한 보안 코드를 생성하며 데이터베이스에 저장하며, 사용자에 의해 작성되는 문서 파일에 보안 코드를 함께 포함시킨다.

[0057] 이를 위해 프로그램 보안 모듈(120)은, 각 사용자의 사용자 군대계급, 사용자 군번, 사용자 소속 부대를 포함하

는 사용자 정보별로 등록된 개인키/공개키 쌍이 존재한다. 또한 문서 암호화를 위한 세션키 및 전자 서명을 위한 임시 개인키/공개키 쌍을 문서별로 생성하고, 문서를 세션키로 암호화하거나 임시 개인키로 전자서명 생성등의 보안 설정을 행한다. 그리고, 보안 설정되는 문서의 구성 정보를 생성하여 등록한다. 또한, 암호화된 문서의 보안 설정 해제를 위해 세션키 및 구성정보를 이용하여 암호화된 문서를 복호화하거나 구성정보에 포함된 임시 공개키(전자 서명 확인키)로 전자 서명을 확인하는 등 보안 문서의 보안 설정을 해제한다. 프로그램 보안 모듈(120)은 모든 파일 I/O를 감시하여, 본 발명에 따른 구성 정보가 존재하는 문서에 대한 파일 I/O를 제어한다.

[0058] 또한 프로그램 보안 모듈(120)은, 등급별로 사용시간 제한을 할 수 있다. 군대내에서는 군사보안 특성상 온라인 게임은 불특정다수와 온라인상에서 채팅(타이핑/보이스), 사행성(결제), 개인정보취급(회원가입) 노출 등의 문제로 현재 이용이 불가한 상태이다. 그러나 본 발명은 이러한 문제를 보안 프로그램을 통해 사전에 차단함으로서 안전하게 온라인 게임을 사용할 수 있는 환경을 제공한다. 또한 암호화된 개인정보 및 장교 등급관리를 통해 사용자의 사용시간을 제한할 수 있어 소수 과다사용 인원 및 다수가 효율적으로 사용 할 수 있어 온라인게임의 부정적 요소를 제거할 수 있다.

[0060] 한편, 군대 내에서 문서 작성이 빈번하게 발생하는데, 문서 파일의 보안의 중요성은 점점 더 증대되고 있다. 국방 문서의 유출은 국가 안보에 중대한 문제를 일으킬 수 있기 때문이다. 이에 클라이언트 단말기(100)에서 작성되는 문서는 암호화되어 저장될 필요가 있다.

[0061] 나아가 군대의 특수성으로 인하여 본 발명은, 아무리 개인 문서 파일이라 하더라도, 본인이 작성한 문서 열람시라도 보안을 위하여 상급 장교의 허가가 있어야 열람 가능하도록 한다. 이에 본 발명은 문서를 읽어들일 때 상급 장교의 인증이 있어야만 문서 열람이 가능하도록 하는 간단한 프로세스를 제공한다. 이하 도 5 및 도 6과 함께 상술한다.

[0062] 도 5는 본 발명의 실시예에 따른 문서 파일의 보안 코드의 저장 예시 그림이며, 도 6은 본 발명의 실시예에 따른 사용자의 상급 장교로부터 문서 파일 인증을 받는 인증창이다.

[0063] 프로그램 보안 모듈(120)은, 로그인한 사용자의 사용자 군대계급, 사용자 군번, 사용자 소속 부대를 포함하는 사용자 정보를 암호화한 보안 코드를 생성하여 데이터베이스에 저장한다. 그 후, 도 5에 도시한 바와 같이, 데이터베이스에 저장된 보안 코드를 제1보안 코드와 제2보안 코드로서 분할하여 제1보안 코드만 사용자에 의해 작성되는 문서 파일에 함께 포함하고, 제2보안 코드는 사용자의 상급 장교의 로그인 정보에 포함시켜 저장한다.

[0064] 그 후, 사용자에 의해 작성되는 문서 파일이 호출될 때 문서 파일에 포함된 제1보안 코드를 추출하고, 사용자의 상급 장교로부터 로그인 승인이 있는 경우에 한하여 제2보안 코드를 추출하여, 추출한 제1보안 코드와 제2보안 코드를 결합하여 보안 코드를 생성하며, 결합 생성한 보안 코드와 프로그램 보안 모듈(120)의 데이터베이스에 있는 보안 코드가 서로 일치하는 경우에만 문서 파일이 표시되도록 한다.

[0065] 즉, 사용자에 의해 작성되는 문서 파일이 호출될 때, 사용자의 상급 장교의 단말기(휴대폰)에 도 6에 도시한 문서열람 인증창이 표시되도록 하여 상급 장교의 로그인 인증이 완료된 경우에 한하여 상급 장교의 로그인 정보에 포함된 제2보안 코드를 추출하여 활용하도록 한다. 만약, 도 6에 도시한 문서열람 인증창에서 인증이 성공되지 못하면, 제2보안 코드가 추출되지 않기 때문에 문서 파일 표시가 되지 않게 된다.

[0066] 참고로, 사용자의 상급 장교의 단말기(휴대폰)를 통하여 상급 장교의 로그인 승인이 있게 되면, 중앙 통제 서버(200)는, 상급 장교의 로그인 정보에 포함된 제2보안 코드와 함께 문서 열람 승인 사실을 클라이언트 단말기(100)로 전송한다.

[0067] 이러한 문서 열람 승인을 통보받은 클라이언트 단말기의 프로그램 보안 모듈(120)은, 수신한 제2보안 코드와 문서 파일에서 추출한 제1보안 코드를 결합하여 프로그램 보안 모듈(120)의 데이터베이스에 있는 보안 코드와 일치하는지를 판정하게 된다.

[0069] 상술한 본 발명의 설명에서의 실시예는 여러가지 실시가능한 예중에서 당업자의 이해를 돕기 위하여 가장 바람직한 예를 선정하여 제시한 것으로, 이 발명의 기술적 사상이 반드시 이 실시예만 의해서 한정되거나 제한되는 것은 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위내에서 다양한 변화와 변경 및 균등한 타의 실시예가 가능한 것이다.

부호의 설명

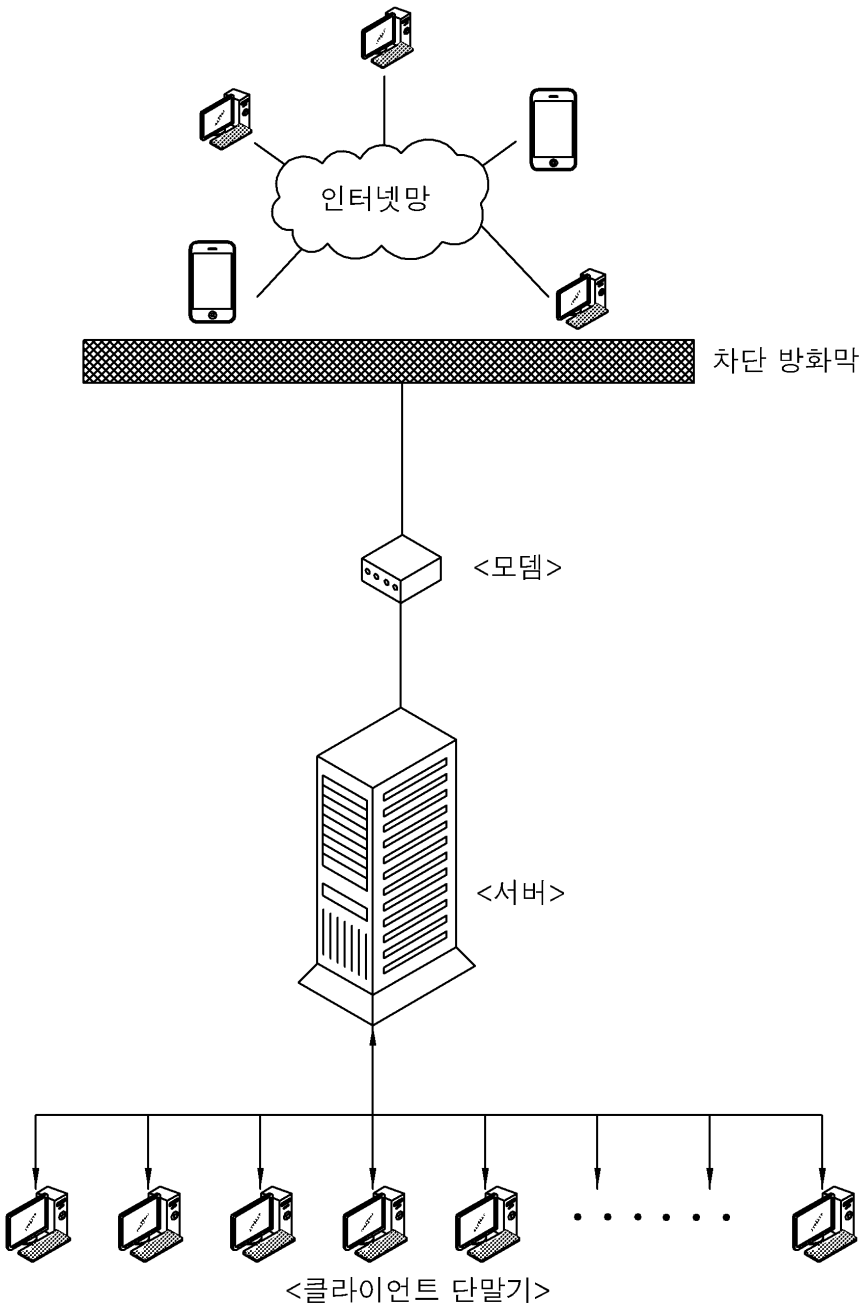
[0071] 100:클라이언트 단말기

200:중앙 통제 서버

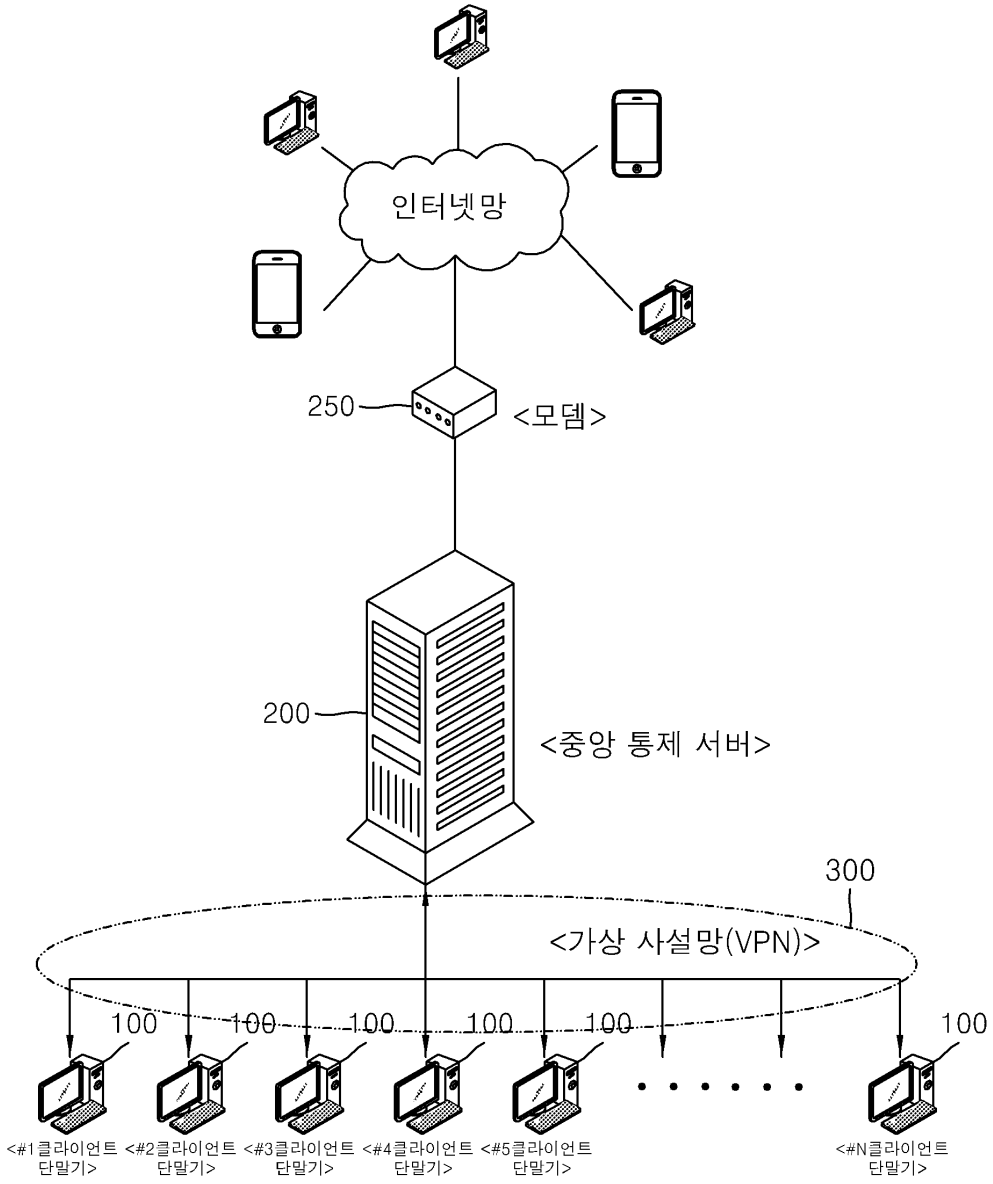
300:가상 사설망

도면

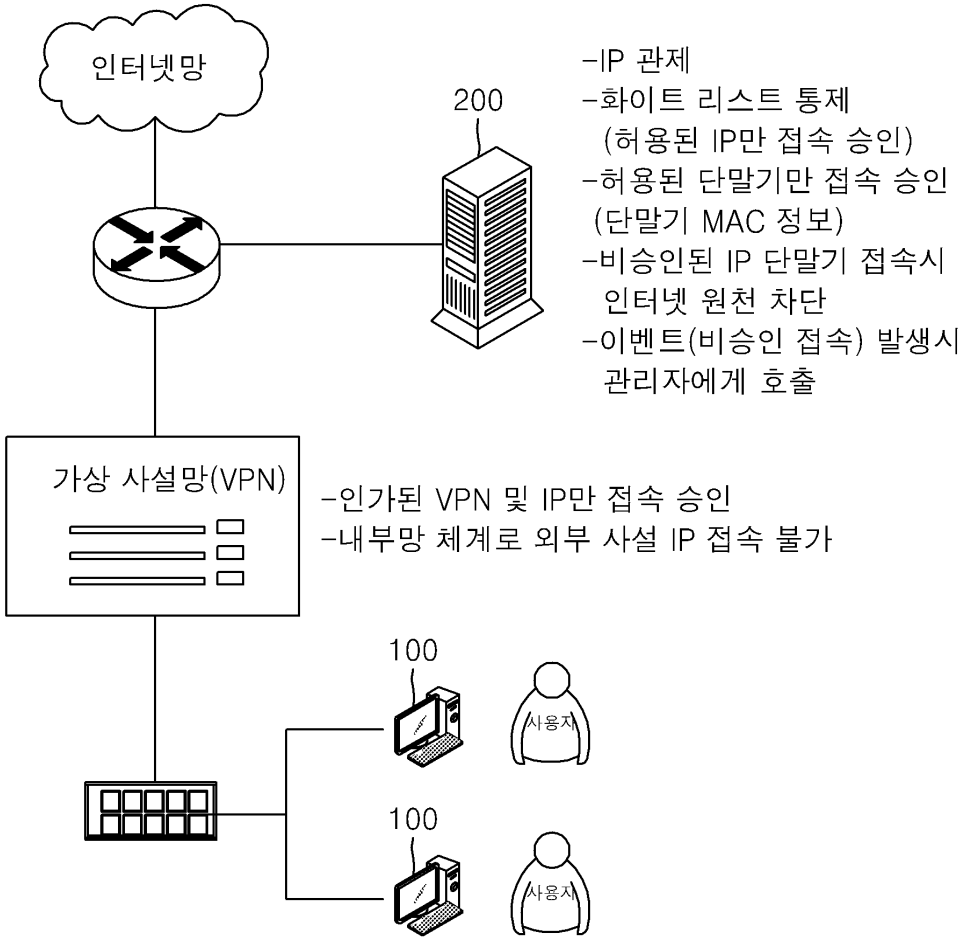
도면1



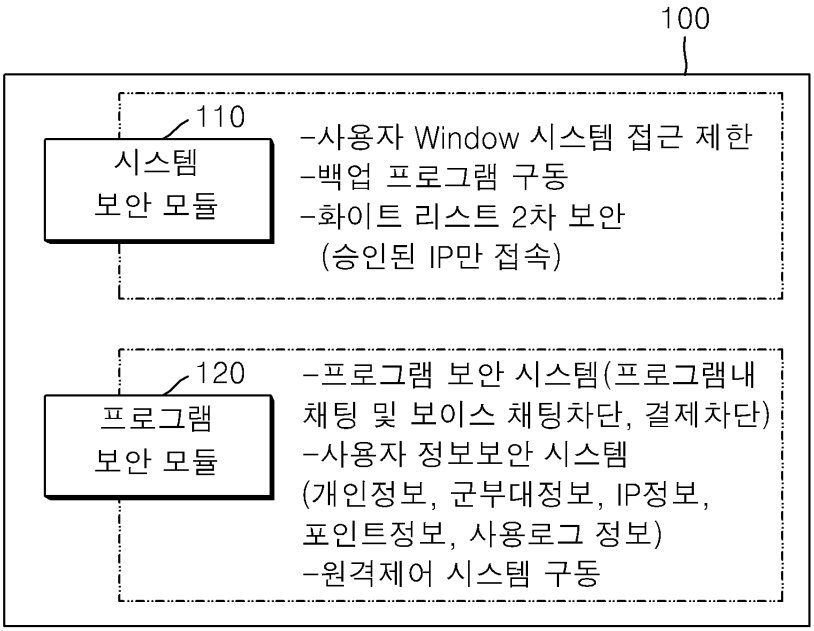
도면2


인터넷망
250
<모뎀>
200
<중앙 통제 서버>
300
<가상 사설망(VPN)>
100
100
100
100
100
100
<#1클라이언트 단말기>
<#2클라이언트 단말기>
<#3클라이언트 단말기>
<#4클라이언트 단말기>
<#5클라이언트 단말기>
<#N클라이언트 단말기>

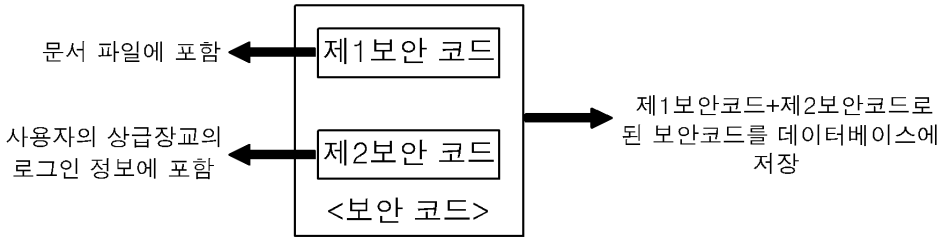
도면3


인터넷망
200
-IP 관제
-화이트 리스트 통제
(허용된 IP만 접속 승인)
-허용된 단말기만 접속 승인
(단말기 MAC 정보)
-비승인된 IP 단말기 접속시
인터넷 원천 차단
-이벤트(비승인 접속) 발생시
관리자에게 호출
가상 사설망(VPN)
-인가된 VPN 및 IP만 접속 승인
-내부망 체계로 외부 사설 IP 접속 불가
100
사용자
100
사용자
-사용자 Window 시스템 접근 제한
-백업 프로그램 구동
-화이트 리스트 2차 보안(승인된 IP만 접속)
-프로그램 보안 시스템
-사용자 정보보안 시스템
-원격제어 시스템 구동

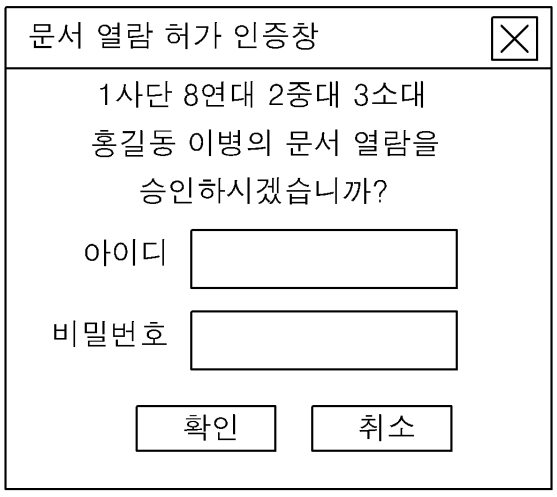
도면4


100
110
시스템
보안 모듈
-사용자 Window 시스템 접근 제한
-백업 프로그램 구동
-화이트 리스트 2차 보안
(승인된 IP만 접속)
120
프로그램
보안 모듈
-프로그램 보안 시스템(프로그램내
채팅 및 보이스 채팅차단, 결제차단)
-사용자 정보보안 시스템
(개인정보, 군부대정보, IP정보,
포인트정보, 사용로그 정보)
-원격제어 시스템 구동

도면5


문서 파일에 포함
제1보안 코드
사용자의 상급장교의
로그인 정보에 포함
제2보안 코드
<보안 코드>
제1보안코드+제2보안코드로
된 보안코드를 데이터베이스에
저장

도면6


문서 열람 허가 인증창
1사단 8연대 2중대 3소대
홍길동 이병의 문서 열람을
승인하시겠습니까?
아이디
비밀번호
확인
취소