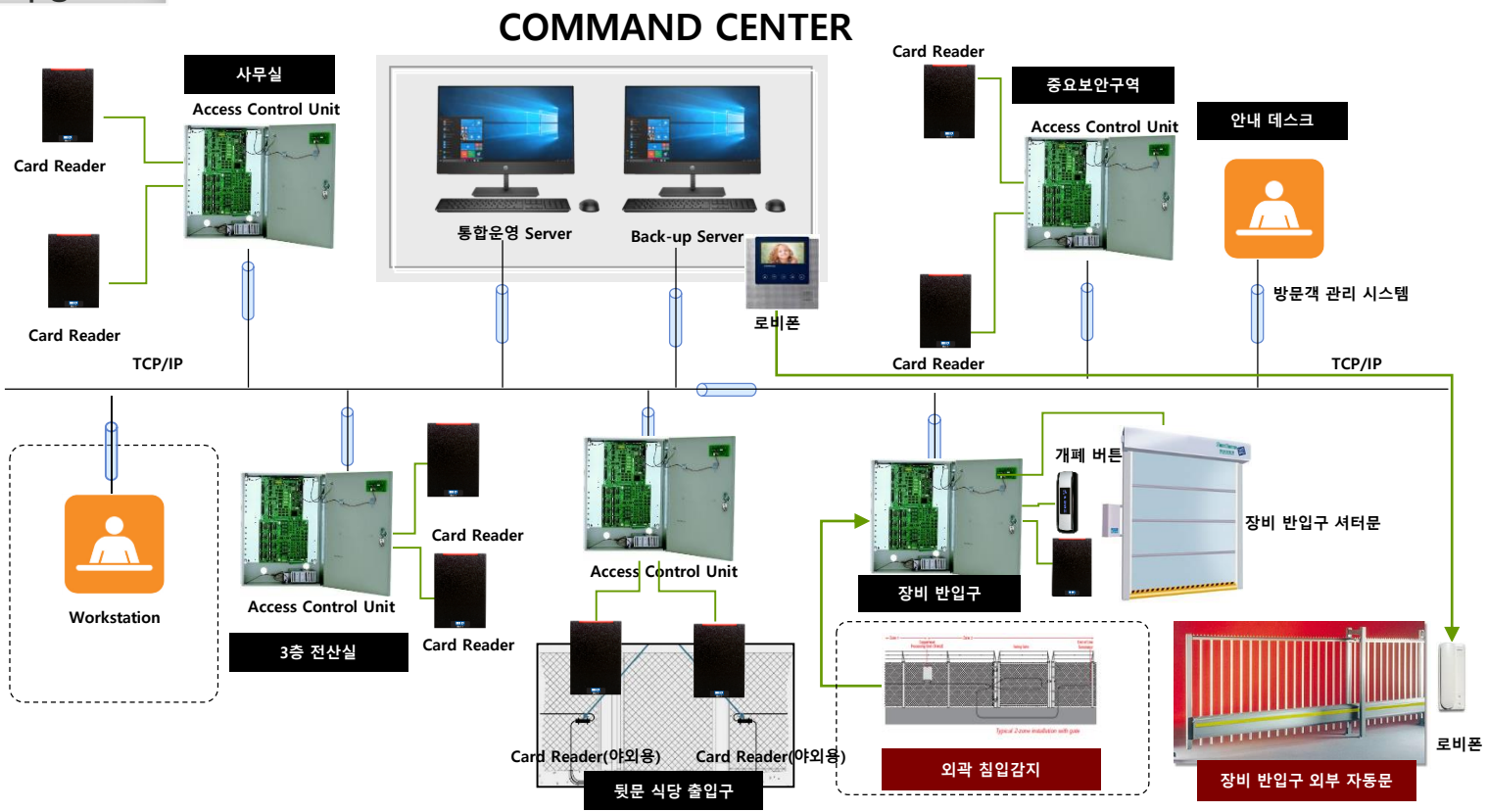
출입통제시스템
교육자료

INDEX

1

출입통제 구성도

출입통제 시스템 구성도



2

출입통제 용어집

*A~Z, ㄱ~ㅎ 순서로 진행

- 1:1 인증: 사용자 자신이 자신임을 확인받는 인증 방법. 개인의 바이오 정보와 데이터베이스에 저장된 바이오 정보를 일대일로 비교하여 검증한다.
- 1:N 인증: 데이터베이스에서 사용자 정보를 찾아내는 인증 방법. 개인의 바이오 정보와 등록된 모든 데이터베이스의 정보를 비교하여 식별하는 방식.
- ANSI 378: 미국 규격 협회(ANSI)에서 정의한 지문 템플릿 표준.
- DHCP: 동적 호스트 설정 통신 규약(Dynamic Host Configuration Protocol)의 줄임말. TCP/IP 통신을 위해 필요한 설정 정보를 자동으로 할당하고 관리하기 위한 통신 규약.
- DIP 스위치: 하드웨어 변경없이 사용자가 회로 기판상에서 기능을 임의로 선택할 수 있는 On-Off 스위치.
- Fail Safe Lock: 전원이 끊기면 안전 상태가 된다는 의미로, 화재 등으로 출입문에 공급되는 전원이 끊겼을 때 잠금이 해제되어 출입문이 개방된다.
- Fail Secure Lock: 전원이 끊기면 보안 상태가 된다는 의미로, 은행과 같이 보안이 중요한 사이트의 출입문 전원이 끊겼을 때 문이 잠긴다.
- Smart 카드: 데이터 읽기와 쓰기가 모두 가능한 13.56MHz 대역의 전자식 카드로, 스마트 카드라고도 한다. 특정 리더만 읽기가 가능하도록 설정하거나 데이터를 암호화하는 등 다양한 보안 기능을 적용할 수 있다.
- HTTP: HyperText Transfer Protocol의 줄임말로, 웹 브라우저를 이용해 웹 클라이언트와 웹 서버가 데이터를 주고받는 프로토콜을 의미한다.
- HTTPS: HyperText Transfer Protocol over Secure Socket Layer의 줄임말로, HTTP보다 보안이 강화된 형태의 프로토콜을 의미한다. HTTPS에서 주고받는 모든 데이터는 암호화 단계를 거치기 때문에 HTTP에 비해 뛰어난 보안성을 갖는다.
- IC 카드: 반도체 기반의 집적 회로를 내장한 카드로, 스마트 카드라고도 한다. IC 카드는 데이터 읽기와 쓰기가 모두 가능하며, 마그네틱 카드에 비해 저장 공간이 크고 내구성이 뛰어나 자석과 접촉해도 데이터가 손상되지 않는다. 또한, 특정 규격의 리더와만 호환되도록 설정하거나 데이터를 암호화하는 등 다양한 보안 기능을 적용할 수 있어 보안성 및 기능성이 높다.
- I/O: 입력(Input)과 출력(Output)의 약어.
- IP 등급: 고체 및 액체에 대한 제품 보호 정도를 규정한 국제 등급.
- ISO 19749-2: 지문의 세밀한 특징점을 이용하여 지문 정보를 표현한 ISO 국제 지문 데이터 형식.
- LAN: 근거리 통신망(Local Area Network)의 줄임말. 건물과 같은 한정된 지역 내에 위치한 컴퓨터, 프린터, 기타 장치 등을 통신선으로 연결하여 상호 작용할 수 있는 망 시스템.
- NC: Normally Closed의 줄임말. 보통의 상태에서는 릴레이가 닫혀 있으나 장치가 작동하면 열리는 동작. 초기에 릴레이가 닫혀 있기 때문에 연결된 회로에 전류가 흐른다.
- NO: Normally Open의 줄임말. 보통의 상태에서는 릴레이가 열려 있으나 장치가 작동하면 닫히는 동작. 초기에 릴레이가 열려 있기 때문에 연결된 회로에 전류가 흐르지 않는다.
- NVR : 네트워크 상에 설치된 카메라나 비디오 장비를 이용해 해당 액세스 포인트에 대해 영상을 녹화하거나 모니터링하고, 발생된 이벤트를 관리할 수 있는 기능.
- RF(Radio Frequency): 라디오 주파수. 원거리 또는 근거리에서 정보를 인식하기 위해 사용하는 주파수.
- RFID: Radio-Frequency Identification의 줄임말로, RF(Radio Frequency)를 이용해 ID를 인식하고 식별하는 기술. 안테나와 칩으로 구성된 RFID 태그에 정보를 저장하며, 이를 RFID 리더로 판독하여 정보를 식별한다.
- RFID 태그: 카드 등의 사물에 부착하여 사람이나 사물의 고유 식별 정보를 저장하는 전자 태그. RFID 리더는 전파를 이용해 태그에 저장된 정보를 무선으로 인식한다. RFID 태그는 일반적으로 소형 프로세서, 메모리, 소형 안테나, 배터리 등으로 구성되며 읽기 및 쓰기 여부, 전지 내장 여부, RF(Radio Frequency) 주파수 대역 등에 따라 여러 종류로 구분한다.

2 출입통제 용어집

*A~Z, ㄱ~ㅎ 순서로 진행

- EXIT 버튼: 내부에서 출입문을 열기 위한 버튼이다. 이 버튼을 누르면 출입문이 열리며, 퇴실할 때 별도의 인증이 필요하지 않은 출입문에 사용할 수 있다.
- RS-485: 홈 네트워크를 지원하는 일종의 시리얼 통신 프로토콜 표준규격. RS-232는 전송속도가 낮고 전송거리가 짧은 반면, RS-485는 모든 장치가 같은 라인에서 데이터 전송 및 수신을 할 수 있다.
- SSL: Secure Socket Layer의 줄임말로, 웹 클라이언트와 웹 서버가 네트워크로 통신할 때 보안과 데이터 무결성을 위해 사용하는 암호 규약을 의미한다.
- TCP/IP: 전송 제어 프로토콜/인터넷 프로토콜(Transmission Control Protocol/Internet Protocol)의 줄임말로, 컴퓨터 간 통신 프로토콜.
- TLS: Transport Layer Security의 줄임말로, 웹 클라이언트와 웹 서버가 네트워크로 통신할 때 보안과 데이터 무결성을 위해 사용하는 암호 규약을 의미한다.
- UHF : 극초단파. 주파수가 300~3000MHz에 속하는 전자기파. 위성방송, 휴대전화 등의 이동 통신, 지상파 디지털 TV, 항공 무선, RFID 기술 등 다양한 통신 분야에서 사용한다. 높은 주파수로 인해 1~10cm의 짧은 파장을 가지며, 직진성이 강한 특징을 갖는다.
- VoIP: IP(Internet Protocol)망을 기반으로 음성 통화를 제공하는 통신 기술.
- Wiegand: 두 개의 신호선 DATA0, DATA1을 이용해 소량의 데이터를 전송하는 방식. 주로 출입 통제 장치의 리더와 컨트롤러 간의 통신 방식에 사용한다.
- 강제 문 열림: 정상적인 출입문 열림 이벤트(사용자 인증, 퇴실 버튼 등)가 발생하지 않고, 출입문 센서가 문 열림을 감지한 상태.
- 개별 인증: 관리자가 지정한 크리덴셜 조합에 따라 사용자를 인증하는 방식으로 다른 인증 방식에 우선한다.
- 개인 식별 번호 (PIN): Personal Identification Number의 줄임말. 본인임을 확인할 수 있도록 개인에게 부여하는 개별 식별 번호.
- 경보: 시스템에서 발생한 알람 이벤트를 실시간으로 보여주거나 전달하는 동작.
- 경비 개시: 범죄 및 안전사고 예방용으로 특정 지역을 감시하는 것. 보안 시스템을 통하여 24시간 감시, 경보 알림, 녹화 등이 가능하다.
- 경비 구역: 경비 개시 후 허가 받지 않은 사람이 침입을 시도할 경우 경고음을 출력하거나 릴레이 신호를 출력하도록 설정한 구역. 주로 업무 종료 이후 경비를 개시하며, 경비 개시 이후 출입을 시도할 경우 설정된 알람이나 신호가 출력된다.
- 경비 해제: 특정 지역에 대한 경보 시스템 가동을 중지하는 것.
- 구역: 출입 규칙의 적용 대상이 되는 장치 그룹. 이벤트를 모니터링하기 위해 사용한다.
- 고급 암호 표준 (AES): 미국 국립 표준 기술 연구소(NIST)가 만든 데이터 암호화 표준(DES)를 대신할 차세대 국제 표준 암호 알고리즘.
- 관리자: 모든 설정 권한을 가진 사용자.
- 광학식 지문 센서: 빛을 이용하여 지문 정보를 검출하는 센서.
- 근거리 무선 통신(NFC): 모바일 단말기에 탑재하여 근거리에서 양방향 데이터 송수신을 지원하는 RFID 기술. 스마트폰 보급률이 늘어남에 따라 금융, 통신 등 다양한 분야에 이용되며, 출입통제 분야에서도 모바일 ID 카드의 형태로 활용되고 있다.
- 노이즈: 신호를 모호하게 하거나 식별하기 어렵게 만드는 전기적 신호.
- 단락: 전선이 합선된 상태. 일반적으로 전선의 손상이나 과전류로 인해 발생한다.
- 단선: 전선이 끊어져 회로가 개방된 것으로, 전류가 흐르지 않는 상태.
- 대역폭: 특정한 기능을 수행할 수 있는 주파수의 범위로, 헤르츠(Hz) 단위로 측정한다. 일정 시간 동안 전선 또는 다른 매체를 통해 전송될 수 있는 정보의 양. 주파수의 대역폭이 클수록 특정 시간 동안 더 많은 정보를 보내는 것이 가능하다.
- 더미 리더: 사용자 데이터 저장이나 판단은 수행하지 않으며, 얼굴, 지문 및 카드 등 크리덴셜 데이터를 읽어 컨트롤 장치로 전송하는 역할만을 하는 장치.
- 도어 컨택: 출입문 센서의 다른 말. 출입문의 현재 상태(닫힘/열림)를 확인하기 위한 자기 센서.
- 동일 오류율: EER(Equal Error Rate). 바이오 인식 성능의 지표이며, 타인 수락률(오인식률)과 본인 거부율(오거부율)이 일치하는 지점의 타인 수락률(오인식률). 일반적으로 낮은 동일 오류율을 가진 장치가 정확하다.

2

출입통제 용어집

*A~Z, ㄱ~ㅎ 순서로 진행

- 로컬 구역: 장치 간 RS-485 통신을 이용해 설정한 구역으로, 해당 구역의 마스터 역할을 서버가 아닌 마스터 장치가 수행한다.
- 릴레이: 전기 회로의 개폐를 다른 전기 회로의 전류, 전압, 주파수 등의 변화에 따라 자동으로 실행하는 제어 기기.
- 마그네틱 카드: 자기 테이프의 자성을 변화시켜 데이터를 저장하는 카드. 카드 한쪽 면의 자기 테이프를 카드 단말기에 읽혀 데이터를 전송한다. 용량이 적고 제한된 종류의 데이터만 저장할 수 있으며, 자석과 접촉하면 기록된 데이터가 변형되거나 손상될 수 있다. 또한, 데이터를 암호화하지 않기 때문에 보안성이 낮아 출입통제 분야뿐만 아니라 다양한 분야에서 IC 카드로 교체되는 추세이다.
- 마스터 장치: RS-485로 연결한 장치 중 컨트롤러 역할을 수행하는 장치. 슬레이브 장치를 주기적으로 모니터링하여 데이터를 처리한다.
- 매칭 타임아웃: 장치 혹은 서버 매칭에 주어지는 제한 시간. 시간 내에 매칭이 완료되지 않을 경우 매칭이 실패된다.
- 멀티 RFID 카드 기술: 125kHz, 13.56MHz와 같이 서로 다른 대역 주파수의 카드를 하나의 장치에서 읽을 수 있는 기술.
- 모바일 카드: 사용자 및 크리덴셜 데이터를 모바일 장치에 저장하여 NFC 또는 BLE 기술을 통해 인증을 수행하는 카드. 모바일 카드는 플라스틱 카드에 비해 높은 보안성과 편의성을 함께 도모할 수 있으며, 거의 모든 사람들이 일상적으로 사용하는 모바일 기기를 이용함으로써 카드 발급 및 관리 비용을 절감할 수 있다는 장점을 갖는다.
- 무선 랜: 무선 주파수(RF) 기술을 이용한 근거리 네트워크. 무선 접속 장치(AP)가 설치된 곳을 중심으로 일정 거리 내에서 WLAN 카드가 장착된 단말기를 이용해 통신망을 이용할 수 있다.
- 무선 접속 장치(AP): Access Point의 줄임말. 무선 랜을 설치하기 위한 중계 장치. 유선 랜을 통해 무선망에 연결하는 역할을 한다.
- 무작위 대입법: Brute-Force Attack(무차별 대입 공격)이라고도 하며, 암호를 풀기 위해 가능한 모든 값을 무작위로 대입하는 것을 의미한다.
- 무정전 전원 공급 장치(UPS): 정전 등의 원인으로 주 전원의 공급이 중단되었을 때 일정 시간 동안 내장된 배터리를 이용해 장치에 비상 전원을 공급해 주는 장치. 통신, 방송, 의료 시설, 데이터 센터, 기간 시설과 같이 전원의 안정적 공급이 필수적인 시설에서 주로 사용한다.
- 바이오 정보: 개인의 신원을 식별할 수 있는 정보. 개인이 가진 고유한 신체적, 행동적 특징을 갖는 정보로 지문, 정맥 패턴, 얼굴, 음성, 홍채, 유전자 등
- 바이오 인식: 사람의 신체적, 행동적 특징을 자동화된 장치로 추출하고 분석하여 개인의 신원을 확인하는 기술. 생체 인식이라고도 한다.
- 바이오 인증: 개인의 바이오 정보와 데이터베이스에 저장된 개인의 바이오 인식 특징을 비교하여 일치 여부를 판단하는 것.
- 반도체식 지문 센서: 다수의 센서를 반도체 위에 배열하여 지문 정보를 전기적으로 검출하는 센서.
- 방수: 우천이나 침수 등으로 인해 장치에 액체가 스며들어 장치 기능에 영향을 주는 것을 방지하기 위한 가공.
- 방화벽: 개인 및 조직의 PC에서 사용하는 네트워크에 허가 받지 않은 외부인이 접근하여 정보를 유출하거나 시스템을 손상시키는 것을 방지하기 위한 보안 시스템. 방화벽은 외부의 인터넷과 내부의 전용 네트워크의 경계에 위치하며, 외부로부터 들어오는 접근 시도를 정해진 접근 규칙에 따라 허용 또는 차단한다.
- 보안 등급: 사용자의 신원을 확인하는 데 필요한 지문의 일치 정도. 보안 수준이 높을수록 본인 거부율이 높아질 수 있다.
- 보안 탬퍼: 장치가 브래킷과 분리되어 탬퍼가 발생할 경우 장치에 저장되어 있는 사용자, 로그, 암호화 키, SSL 인증서에 대한 모든 정보가 즉시 삭제되도록 하는 기능.
- 복호화: 암호화된 데이터를 복호화 키를 이용해 원래대로 복원하는 것. 암호화된 데이터는 암호화에 사용된 키와 쌍을 이루는 대칭키로만 복호화가 가능하다.
- 본인 거부율 (오거부율): FRR(False Rejection Rate). 바이오 인식 시스템의 정확성을 비교하는 데 사용되는 기준으로서 등록자를 비등록자로 인식할 확률.
- 블루투스(Bluetooth): 근거리에서 양방향 데이터 송수신을 지원하는 통신 기술. 전송 거리, 전송 방식, 전원 소모량 등에 따라 각각 다른 특징을 갖는다.
- 비접촉식 카드:카드에 내장된 코일 안테나를 이용해 카드 단말기와 통신하는 카드. 카드 단말기와 접촉 없이 자기장을 이용해 데이터를 전송할 수 있다.

2

출입통제 용어집

*A~Z, ㄱ~ㅎ 순서로 진행

- 생활 방수: 방수보다는 다소 낮은 수준의 방수 성능.
- 서버: 서버 프로그램이 실행되는 컴퓨터 또는 다른 프로그램에 서비스를 제공하는 컴퓨터 프로그램.
- 서버 매칭: 서버에 저장된 크리덴셜 정보와 사용자가 입력한 크리덴셜 정보를 비교하는 기능.
- 서버 모드: 서버와 장치를 연결할 때 장치에서 서버IP 주소를 직접 입력하는 방식. 직접 입력 방식이기 때문에 장치가 다른 서버나 클라이언트에 잘못 연결될 위험이 없고, 연결이 끊기는 경우에도 자동으로 재연결되므로 안정적인 네트워크 환경을 구성할 수 있다.
- 센서 감도: 지문 이미지를 정확하게 검출할 수 있는 정도. 감도가 높을수록 지문 이미지를 쉽게 얻을 수 있지만 잡음에 대한 민감도도 함께 높아지게 되어 정확한 이미지 검출이 어려울 수 있다.
- 소프트웨어 개발 키트 (SDK): Software Development Kit의 줄임말. 소프트웨어 개발자가 특정한 소프트웨어 프레임워크, 하드웨어 플랫폼, 컴퓨터 등을 위한 응용 프로그램을 만들 수 있게 하는 개발 도구의 집합이다.
- 수축 튜브: 열을 가하면 수축하는 튜브 형태의 고무 탄성체. 주로 전자 제품의 케이블을 단선, 부식, 침수 등으로부터 보호하기 위해 사용한다.
- 스마트 카드: 데이터 읽기와 쓰기가 모두 가능한 13.56MHz 대역의 전자식 카드로, 특정 리더만 읽기가 가능하도록 설정하거나 데이터를 암호화하는 등 다양한 보안 기능을 적용할 수 있다.
- 스캔: 지문 정보를 디지털 데이터로 전환하기 위해 센서 표면에 손가락을 대거나 일정한 속도로 움직이는 동작.
- 슬레이브 장치: RS-485로 연결한 장치 중 리더 또는 입출력 기능만 수행하는 장치. 사용자 정보를 갖고 있지 않으며 마스터 장치에 의해 제어된다.
- 시리얼 통신: 여러 개의 비트를 순차적으로 전송하는 통신 방법. 대표적으로 RS-232와 RS-485가 있다.
- 아날로그 인터폰: 아날로그 교환기와 회선망으로 구성된 인터폰.
- 안티패스백: 출입 통제를 위한 구조적인 방법으로서 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야하는 기능. 카드를 사용해 출입할 때 리더에 카드를 인식시키지 않고 앞사람을 따라 입실했다면 퇴실할 때 출입문이 열리지 않으며, 안티 패스백 이벤트가 발생한다. 안티 패스백은 Hard APB와 Soft APB로 나뉜다. 안티 패스백 위반 시 Hard APB는 안티 패스백 이벤트를 생성하고 출입할 수 없으며, Soft APB는 안티 패스백 이벤트를 생성하고 출입이 가능하다.
- 암호화: 원래 의미를 알 수 없도록 정보를 변환하는 것. 암호화된 형태로 정보를 저장하거나 전송함으로써 정보를 보호할 수 있다.
- 암호화 키: 암호화를 위해 생성된 임의의 비트 문자열. 암호화 키는 모든 키를 예측할 수 없도록 고안된 알고리즘으로 설계되며, 일반적으로 암호화 키가 길수록 해독이 어려워진다.
- 얼굴 인식: 사람의 얼굴 특징을 이용하여 신원을 확인하는 기술 또는 그러한 인증 체계.
- 에폭시: 장치를 옥외에 설치할 경우 빗물이 장치에 들어가는 것을 방지하여 회로를 보호하기 위해 사용하는 소재.
- 위조 얼굴 감지(LFD) 기술: 마스크나 사진 등의 위조 얼굴을 감지하는 기술.
- 위조 지문: 타인의 지문을 본떠서 종이, 실리콘, 고무 등으로 만든 가짜 지문.
- 위조 지문 감지(LFD) 기술: 고무, 실리콘, 점토, 접착제, 필름 등으로 복제한 위조 지문을 감지하는 기술.
- 융선: 지문을 나타내는 하나의 지문 곡선으로서 연속되는 융선과 중간에 끊어지는 끝점, 2개의 융선이 만나는 분기점으로 되어 있으며, 이들을 특징점이라함.
- API : 웹 애플리케이션을 개발할 때 다른 서비스 플랫폼에 요청을 보내고 응답을 받기 위해 정의된 명세. 응용 프로그램에서 사용할 수 있도록 운영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스. 주로 파일 제어, 장 체어, 화상 처리, 문자 제어 등을 위한 인터페이스를 제공한다.
- 이중 인증: 제한된 시간 안에 서로 다른 두 사람의 크리덴셜을 순차적으로 입력하는 인증 방식.
- 인증: 사용자가 입력한 크리덴셜을 검증하여 신원을 판별하는 동작.

2 출입통제 용어집

*A~Z, ㄱ~ㅎ 순서로 진행

- 인증 모드: 인증을 위해 필요한 크리덴셜의 조합.
- 인터락 구역: 두 개 이상의 출입문 사이에 있는 공간으로, 하나의 출입문이 열려 있거나 잠금 해제된 경우 나머지 출입문은 잠기는 구역.
- 인터폰: 보통 한 건물이나 기관 안에 사설 구내 교환기(PBX)를 이용하여 구축한 통신 시스템.
- 입출력 장치: 정보 입출력 기능을 수행하는 장치.
- 잠금 장치: 출입 통제 시스템과 연결되어 출입문을 잠그는 데 사용되는 전자 장치. 출입문에 내장되었거나 장착된 전자 장치를 통칭한다.
- 저전력 블루투스(BLE): 약 10m 내외의 거리에서 2.4GHz 주파수를 이용해 저전력 저용량 데이터를 송수신할 수 있는 블루투스 기술. 저전력 블루투스 기술은 전력 공급이 제한되는 소형 장치에 주로 사용되며, 출입통제 분야에서도 모바일 ID 카드의 형태로 활용되고 있다.
- 접촉식 카드: 표면에 금색 또는 은색의 칩이 부착된 카드. 데이터 전송을 위해서는 카드 단말기에 칩이 직접 접촉되도록 삽입해야 한다.
- 종단 저항: RS-485 데이지 체인의 종단에 위치한 장치에 연결하는 저항. 데이지 체인의 연결이 길어질수록 종단에서 신호 반사가 발생하여 전류의 흐름을 방해하는데, 이 반사를 억제하고 좋은 신호 품질을 얻기 위해 데이지 체인 종단에 연결된 장치에 저항을 연결한다.
- 지능형 카드 리더: 사용자 정보, 출입 정보를 저장하고 입력된 크리덴셜을 인증하여 사용자 출입을 허가할 수 있는 장치.
- 지문: 손가락 끝 마디에 있는 곡선 모양의 무늬.
- 지문 센서: 지문 인식 기술에서 사람마다 고유의 특성 차이를 나타내는 손가락 지문의 영상 정보를 획득하는 입력 영상 장치 또는 지문 스캐너에서 지문 정보를 읽을 수 있도록 손가락을 올려놓는 부분.
- 지문 스캐너: 사용자의 지문을 데이터베이스에 등록하기 위해 지문을 스캔하는 장치.
- 지문 인식: 사람마다 고유한 특성을 가진 손가락 지문의 영상 정보를 이용하여 사람을 인식을 기술 또는 그러한 인증 체계.
- 지문 템플릿: 지문 이미지에서 발견되는 융선의 끝점이나 분기점 등 일련의 세밀한 특징점을 모은 지문 정보. 특징점의 위치와 개수를 비교하여 식별에 사용
- 차폐 연선: 외부의 노이즈를 차단하거나 전기적 신호의 간섭을 줄이는 차폐막으로 감싼 케이블. 신호 간섭이 많은 공장이나 야외, 또는 통신 시 빠른 속도가 필요한 곳에 주로 사용한다.
- 청정실: 먼지, 바이러스, 금속 가루, 세포 등 공기 중 부유 입자를 필요에 따라 제어할 수 있는 공간.
- 초기화: 하드웨어나 소프트웨어의 설정 등을 지정한 초기값으로 되돌리는 일.
- 최대 전송 단위 (MTU): Maximum Transmission Unit의 줄임말. 네트워크를 통해 전송할 수 있는 최대 패킷 양.
- 최상위 비트 (MSB): Most Significant Bit의 줄임말. 2진수 데이터에서 가장 높은 자리(가장 왼쪽)의 비트나 그 내용. 최하위 비트 (LSB)와 반대.
- 최하위 비트 (LSB): Least Significant Bit의 줄임말. 2진수 데이터에서 가장 낮은 자리(가장 오른쪽)의 비트나 그 내용. 최상위 비트 (MSB)와 반대.
- 출력 릴레이: 다른 장치에 영향을 주기 위해 전기적 접촉을 열거나 닫는, 전자적으로 제어되는 장치.
- 출입: 특정 구역 또는 자산에 접근하는 행위.
- 출입 규칙: 특정 출입문/출입문 그룹에 정해진 스케줄 동안 출입할 수 있는 규칙.
- 출입 그룹: 정해진 출입문/출입문 그룹에 정해진 스케줄에 출입할 수 있는 권한을 가진 사용자 그룹.
- 출입 등급: 지정한 스케줄 동안 출입문에 출입할 수 있는 권리.
- 출입 제한 구역: 특정한 시간대에 출입을 제한하는 구역. 인증 또는 인증 횟수를 제한하는 방식으로 구성할 수 있다.
- 출입 통제: 허가되지 않은 사람이 제반 시설이나 자산에 접근하는 것을 제한하는 것. 허가된 사람일 경우 로그를 통해 기록이 생성된다.
- 출입문 그룹: 관리의 용이성을 위한 출입문 집합이며, 출입문 그룹 단위로 이벤트를 감시할 수도 있다. 출입 그룹의 구성 요소.
- 출입문 센서: 출입문 상태를 탐지하는 센서. 열림, 닫힘, 열려 있음, 강제 열림 등의 상태를 확인할 수 있다.

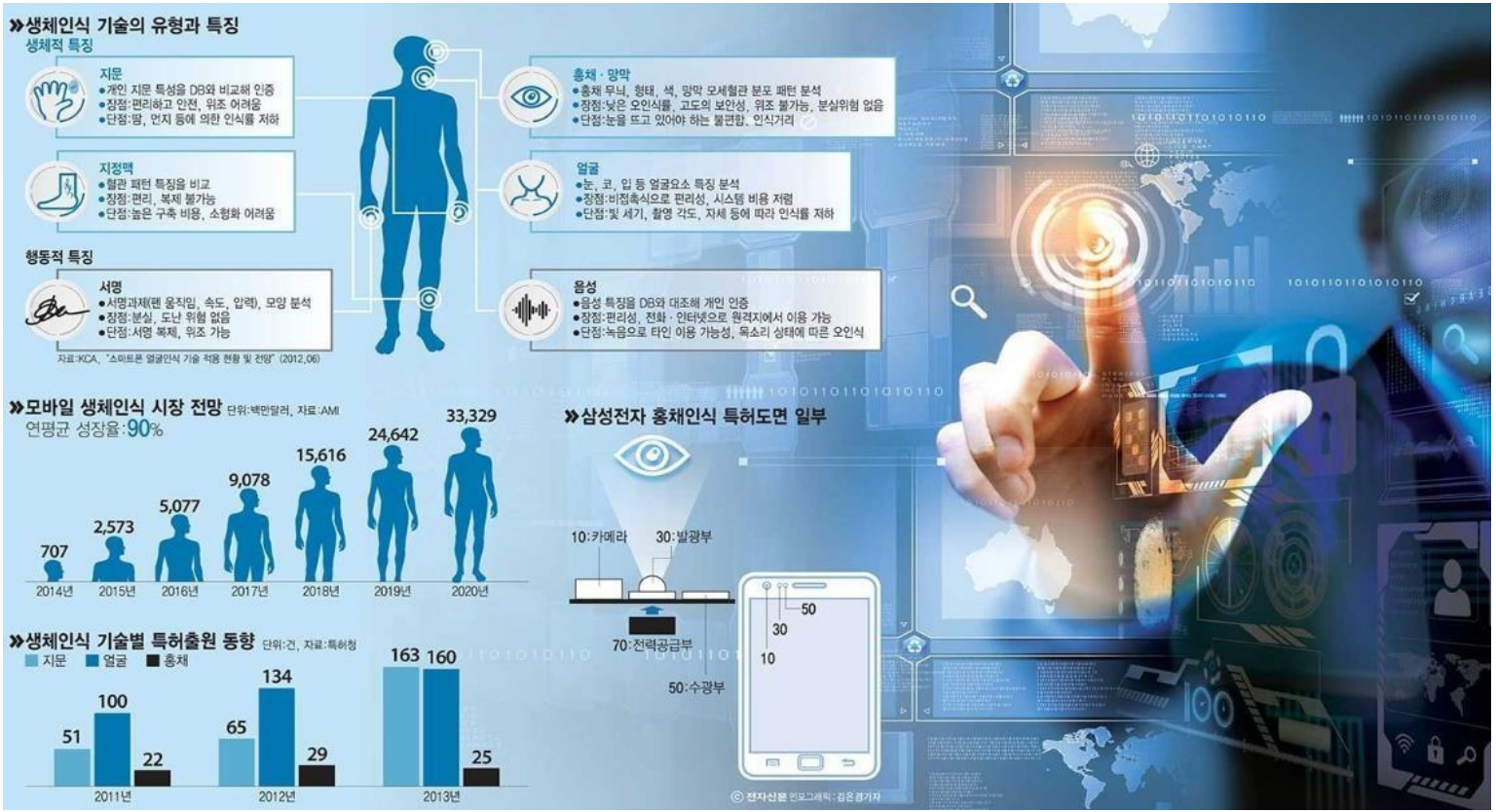
2

출입통제 용어집

*A~Z, ㄱ~ㅎ 순서로 진행

- 카드: 휴대 가능한 카드 모양의 정보 매체로서 신분 증명을 위한 정보가 저장되어 있다.
- 카드 ID: 회사와 조직, 부서에서 정의한 형식에 따라 부여된 카드의 고유 번호. 카드 ID는 카드 제조사에서 부여한 카드의 고유 번호 또는 특정 회사나 조직에서 정의한 형식의 번호가 될 수 있다.
- 카드 일련 번호 (CSN): Card Serial Number의 줄임말. 제조사가 부여한 카드의 고유 번호.
- 컨트롤러: 리더에서 획득한 크리덴셜 정보를 이용하여 출입 권한을 판별하고 리더의 입출력을 제어하는 장치.
- 크리덴셜: 사용자의 신원을 확인하기 위한 데이터. 일반적으로 디지털 서명, 스마트카드, 바이오 정보, 사용자 이름과 비밀번호 등이 있다.
- 클라이언트: 네트워크를 이용해 서버에 서비스를 요청하는 주체.
- 타인 수락률 (오인식률): FAR(False Acceptance Rate). 바이오 인식 시스템의 정확성을 비교할 때 사용되는 기준 비등록자를 등록자로 잘못 인식할 확률.
- 탬퍼: 외부 요인에 의해 장치가 설치된 브래킷에서 분리될 경우 경보가 울리거나 서버에 이벤트가 기록되게 설정할 수 있다.
- 템플릿: 바이오 특징을 추출한 후 부호화하여 저장한 데이터로서, 바이오 인식 시스템 또는 장치에서 사용자가 입력한 바이오 샘플과 비교하여 신원을 파악하는 데 사용됨.
- 퇴실 버튼: 출입문을 열기 위한 버튼. 이 버튼을 누르면 출입문이 열리며, 별도의 인증이 필요하지 않은 출입문이나 구역에 사용할 수 있다.
- 특징점: 지문을 인식하는 데 사용되는 융선의 세밀한 특징적 요소들.
- 펌웨어: 제품의 하드웨어를 제어하기 위해 롬(ROM)에 저장한 마이크로 프로그램 및 파일.
- 포트 번호: TCP/UDP에서 상호 통신하기 위해 사용하는 포트 번호. 범위는 0~65535이다.
- 프로토콜: 시스템 또는 단말기 사이에 데이터를 교환하기 위해 사용하는 통신 규칙.
- 마스터 카드: 인증 절차를 우회하여 특정 지역에 접근할 수 있는 카드. 예를 들면, 이 카드를 소지한 사람은 일련의 보안(인증) 절차를 거치지 않고 출입문을 통과할 수 있다.
- 화재 경보 구역: 화재가 발생할 경우 모든 출입문 또는 엘리베이터가 개방되거나 잠기도록 설정한 구역.

Biometrics 출입보안시스템 주요 현황(전자신문 보도자료 中)



3
출입통제
시스템
설계 방안

출입보안시스템 고도화 방안

FEMA426 보안 기준 출입보안시스템은 위험(Risk)의 양을 측정하고 관련된 설계와 설비를 위한 몇 가지 방법론을 제시하며 원하는 수준의 보호수준까지 수용 가능한 비용으로 가장 효과적으로 취할 수 있는 위협감소 방법을 제안 드립니다.

레벨 1 : 기계식 출입 보안 관리

시건장치 등의 기계식 잠금장치를 이용하여 출입문을 통제하는 단계(전형적인 출입통제 방식)

레벨 2 : 전자식 출입 보안관리

독립형 전자식 도어락을 사용한 출입통제 및 출입보안을 하는 단계(프로그램 기반 전자식 도어락)

레벨 3 : 네트워크 및 IOT 출입통제 관리

네트워크 기반 출입통제 및 RFID 및 IOT활용을 통한 통합보안관리 단계

레벨 4 : Biometrics의 융합 출입통제 관리

지문인식, 정맥인식, 홍채인식, 얼굴인식 등 바이오인식을 통한 개별화 및 통합 고도화 단계

FEMA426 의거 메뉴얼

	사회적 재난			자연적 재난	
	폭발물 테러	방화	생화학 테러	지진	태풍 및 홍수
위험도 평가	**FEMA 452** : Risk Assessment/ A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings **FEMA 455** : Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risk			N/A	N/A
	FEMA_BIPS 04 : Integrated Rapid Visual Screening of Buildings				
건물 설계 가이드	**FEMA 427** : Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks **FEMA 430** : Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks **FEMA 453** : Safe Rooms and Shelters: Protecting People Against Terrorist Attacks **FEMA 459** : Incremental Protection for Existing Commercial Buildings from Terrorist Attack: Providing Protection to People and Buildings			**FEMA 389** : Primer for Design Professionals: Communicating with Owners and Managers of New Buildings on Earthquakes **FEMA 454** : Designing for Earthquakes **FEMA P-749** : Planning Earthquake Resistant Design Concepts **FEMA P-750** : NEHRP Recommended Seismic Provisions for New Buildings and Other Structures	**FEMA 543** : Design Guide for improving Critical Facility Safety from Flooding and High Winds
매뉴얼	**FEMA 426/BIPS 06** : Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, 2nd			N/A	N/A

3 출입통제 시스템 설계 방안

사회적 이슈 사항

서울 **확진자** 중 퇴원자 절반 돌파…첫 환자 확진 89일만
연합뉴스 | 23시간 전 | 네이버뉴스

21일 오전 10시 기준 **확진자** 누계 626명 중 315명 퇴원 서울에서 발생한 코로나19 **확진자** 중 퇴원자의... (마포구 **23번** 환자)과, 가양1동의 자녀 집에 머무르던 부산 해운대구 주민인 83세 남성(강서구 26번 환자)이다....

└ 서울 **확진자** 중 퇴원자 절반 돌파…… SBS | 23시간 전 | 네이버뉴스
└ 서울 **확진자** 2명 늘어난 626명…퇴… 이데일리 | 22시간 전 | 네이버뉴스
관련뉴스 전체보기›

서울 코로나19 **확진자** 전일 대비 2명 늘어 총 626명 TBS | 23시간 전

추가 확인된 마포구 **23번 확진자**는 미국에서 지난 18일 오후에 입국한 20대 남성으로, 어제(20일) 오전 양성 판정을 받고 서울적십자병원으로 옮겨졌습니다. 또 다른 신규 확진자인 강서구 26번째 확진자는 강서구...

서울시는 왜 추가 **확진자** 2명인데 0명이라고 발표했나
뉴시스 | 1일 전 | 네이버뉴스

곧이어 마포구에서도 '마포구 **23번 확진자** 동선 안내'를 통해 관내 23번째 확진자가 이날 오전 9시 확진판정을 받았다고 발표했다. 서울시 기준대로라면 코로나19 확진환자는 '0명'이 아니라 '2명'이 돼야 맞지만...

└ 서울시는 왜 추가 **확진자** 2명인데 0… 톱스타뉴스 | 1일 전

코로나 **확진자** 13명 증가, 22일 생활방역 지침 발표 경상일보 | 1일 전

울산에서는 20일 오후 현재까지 추가 **확진자**가 발생하지 않았다. 이날 재양성판정을 받은 울산 **23번** 환자가 완치 판정을 받고 퇴원했다. 울산지역 코로나 **확진자**는 총 43명이다. 총 35명이 완치해 퇴원했고, 1명이...

아무리 방지를 해도 문제가 발생됩니다.

건물입구에서부터 차단 할 수 없을까요?

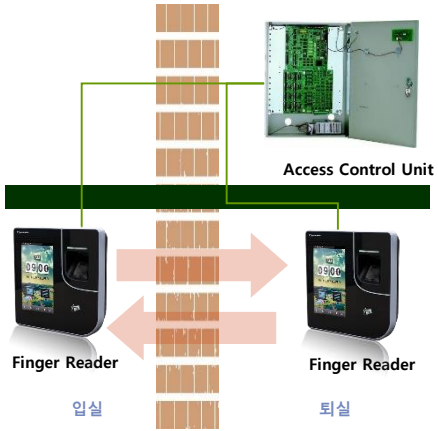
'고가의 열화상 카메라도 품절현상' - OO일보 -
"코로나19 증상, 열 마른기침 목아픔 두통..자가격리 추천"

중국 '우한'서 온 23번 확진자, '소재불명' 상태서 14일간 외부에 노출

3
출입통제
시스템 변화

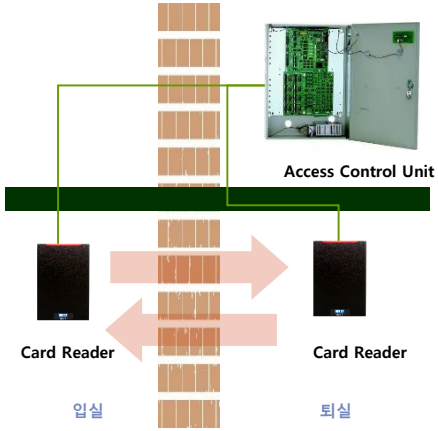
단계별 차등으로 특별지역의 물리보안 강화

출입보안 1등급 구역



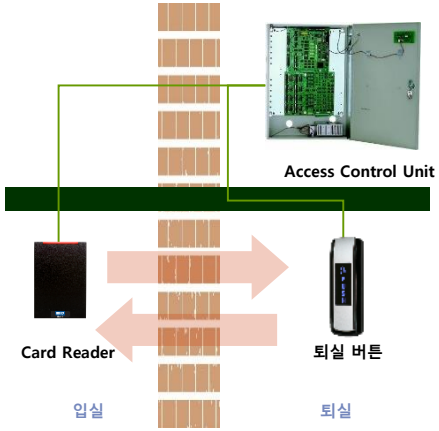
- Anti-Pass back 기능 적용
  - 입-퇴 교번 규칙을 적용하여 입실과 퇴실의 정확한 기록을 유지 및 관리
- 입실 : 지문인증
- 퇴실 : 카드인증
- 적용장소 : 각 층 입주사 전산실

출입보안 2등급 구역



- Anti-Pass back 기능 적용
  - 입 / 퇴 교번 규칙을 적용하여 입실과 퇴실의 정확한 기록을 유지 및 관리
- 입실 : ID카드인증
- 퇴실 : ID카드인증
- 적용장소 : 외부 -> 내부로 통하는 출입문, 각 층 엘리베이터 홀

출입보안 3등급 구역



- 일반적인 출입통제 형태로 구성
- 입실 : ID카드인증
- 퇴실 : 퇴실 버튼
- 적용장소 : 출입이 비교적 자유로운 일반 사무실

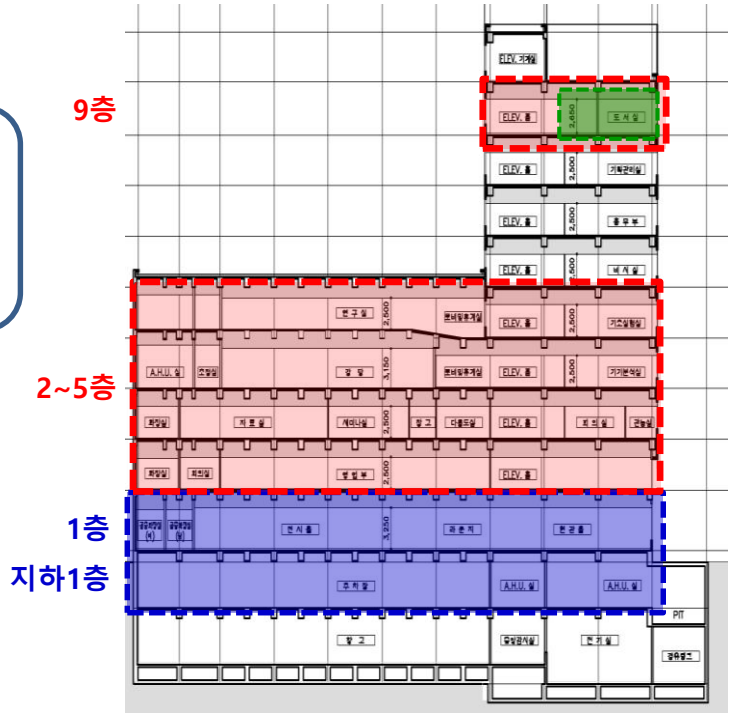
3 출입통제 시스템 설계방안

다양한 시설의 보안시스템 설계 효율성

단계별 출입통제 방안

- 1차 통제 구역
  - 1층 로비, 지하1층 계단
    - 내부로 진입하는 관문으로 출입이 허가된 자만이 출입 가능함
    - 방문객은 안내데스크를 통하여 출입허용

- 2차, 3차 통제 구역
  - 업무시설
    - 1차 통제구역을 통과한 인원에 보안구역의 출입을 단계적으로 제한함
    - 방문객은 피 방문자의 인솔하에 업무시설로 진입허용



단계별 출입통제 및 감시

- 주출입구, 비상계단실 입구, 내부 주요시설에 대해 출입통제 장치 설치
- 외부인원 및 불필요한 인원에 대해서는 철저한 확인과 차단
- 단계별 규제 및 확인을 통해 출입인원의 정확한 신원 및 위치 정보 확보

내부 임직원의 불편함 최소화

- 1층 로비 엘리베이터 홀에 스피드게이트 설치
- 내부임직원에 대해서 보안등급별, 업무별 출입구획을 별도 지정하여, 보안성을 높임과 동시에 임직원의 보안의식 고취

3 출입통제 시스템 설계방안

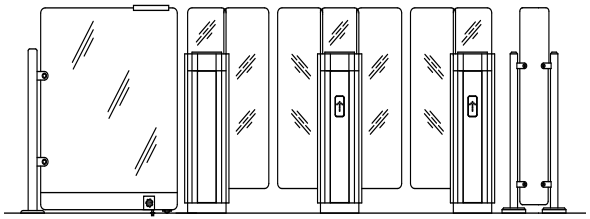
다양한 시설의 보안시스템 설계 효율성

로비 / 비상계단

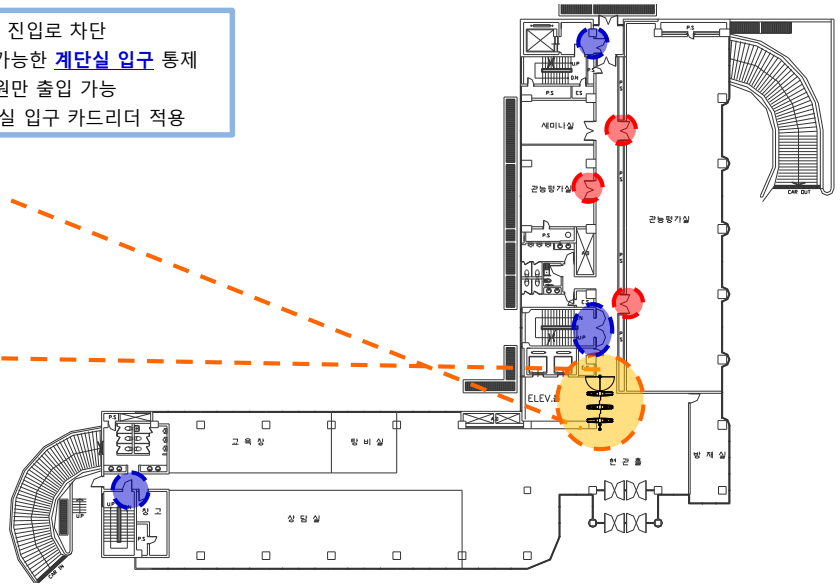
1층 로비 **엘리베이터 홀** 진입차단
- 출입이 허가된 인원만 출입 가능
- 스피드게이트 적용으로 효율적 인원관리

사무실 입구 진입차단
- 출입이 허가된 관련부서 직원만 출입 가능
- 1층 사무실 카드리더 적용

외부에서 건물 내부로의 진입로 차단
- 상부층으로 이동 가능한 **계단실 입구** 통제
- 출입이 허가된 인원만 출입 가능
- 1층, 지하1층 계단실 입구 카드리더 적용



[내부]



3 출입통제 시스템 설계방안

다양한 시설의 보안시스템 설계 효율성

2차 통제 구축 방안

비상계단을 통한 업무시설 지역으로의 진입로 차단

- 업무시설로 이동 가능한 계단실 출구 통제
  (계단실에서 업무공간으로 진입은 카드리더로 차단,
  업무공간에서 계단실 진입은 퇴실버튼 적용)
- 1차 통제지역을 통과하였더라도 허가된 층의 직원만 출입 가능
- 1~5층, 9층 계단실 출구 카드리더 적용

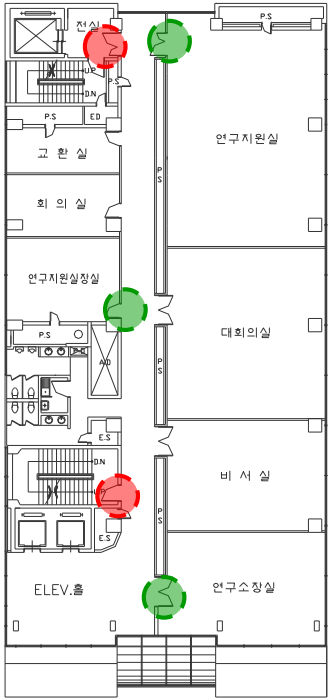
3 출입통제 시스템 설계방안

다양한 시설의 보안시스템 설계 효율성

3차 통제 구축 방안

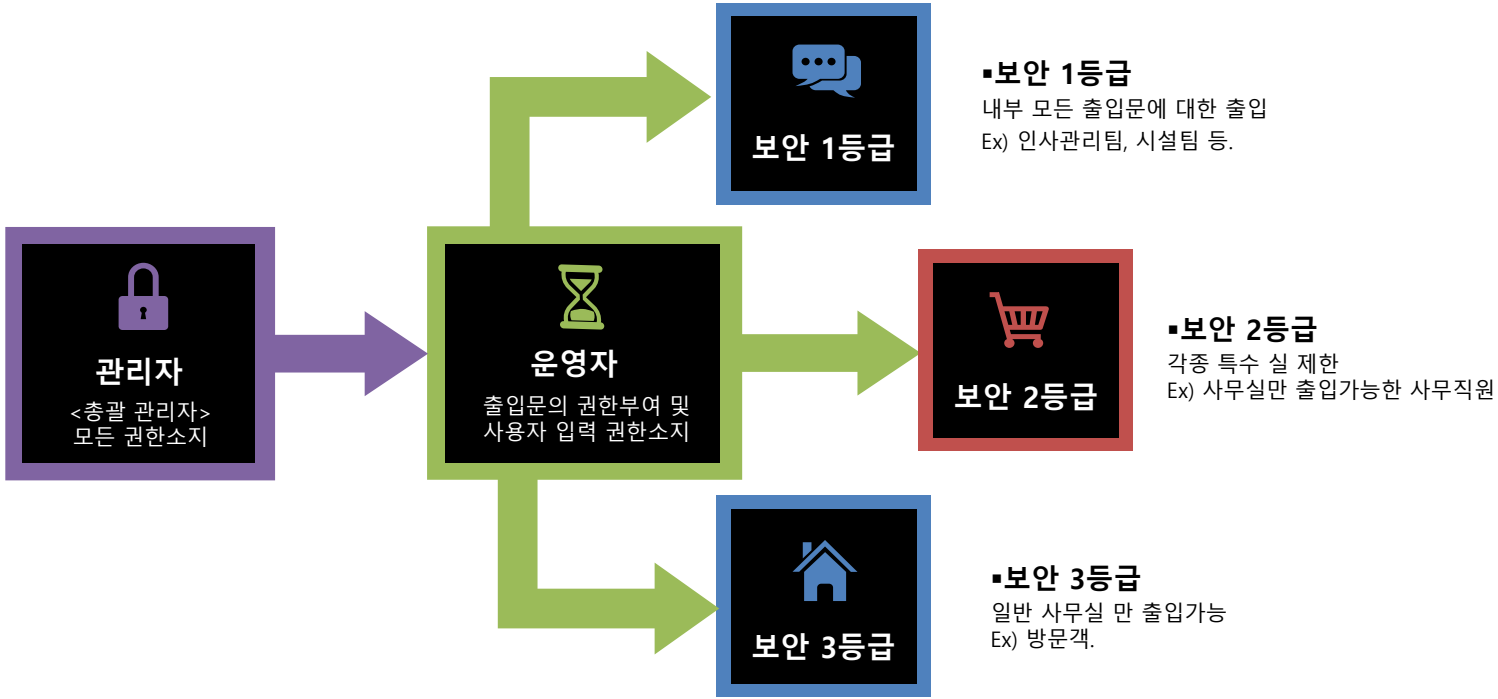
중요 사무실 진입 차단
- 1,2차 통제지역을 통과하였더라도 허가 받은 인원만 진입가능
- 9층 사무실 출구 카드리더 적용

비상계단을 통한 업무시설 지역으로의 진입로 차단
- 업무시설로 이동 가능한 **계단실 출구** 통제
  (계단실에서 업무공간으로 진입은 카드리더로 차단,
  업무공간에서 계단실 진입은 퇴실버튼 적용)
- 1차 통제지역을 통과하였더라도 허가된 층의 직원만 출입 가능
- 1~5층, 9층 계단실 출구 카드리더 적용



3 출입통제 시스템 설계방안

보안 구역 접근 규칙



▪보안 1등급
내부 모든 출입문에 대한 출입
Ex) 인사관리팀, 시설팀 등.

▪보안 2등급
각종 특수 실 제한
Ex) 사무실만 출입가능한 사무직원

▪보안 3등급
일반 사무실 만 출입가능
Ex) 방문객.

<예시> 자체 내규에 의거 적용

3 출입통제 시스템 설계방안

보안 구역 접근 규칙

방문신청

- ✓ 방문자는 구축된 방문객 관리 시스템에 접속하여 관련된 방문사항을 입력
- ✓ 입력된 방문자 정보는 안내 Desk에 설치된 보안관리 Workstation에 전송

외부인의 출입을 선별하여 허가함으로써 내부 보안 강화

방문객 DB 전송

- ✓ 방문객 전용 카드는 공통 출입구(메인로비, 1층 엘리베이터홀)에 대해서는 사전 출입권한이 부여
- ✓ 방문 출입구에 대해서는 안내 Desk관리자에 의해 출입권한이 부여

방문카드유효기간 설정을 통해 철저한 방문객 출입관리

이력 관리

- ✓ 방문객 출입과 관련된 모든 정보는 통합보안관리 서버에 전송
- ✓ 전송된 방문객 관리정보는 저장 및 레포트로 출력이 가능

방문자 데이터 관리를 통한 향후 문제 발생 시 즉각적인 대응

카드 설정

- ✓ 상주직원카드
- ✓ 임시 출입카드
- ✓ 방문객 카드
- ✓ 제한 기능의 임시 카드
- ✓ 제한 기능의 방문자 카드

인증된 통행자를 뒤따라 무단으로 들어오는 비 인증자 완벽하게 차단

3 출입통제 시스템 설계방안

보안 구역 접근 규칙

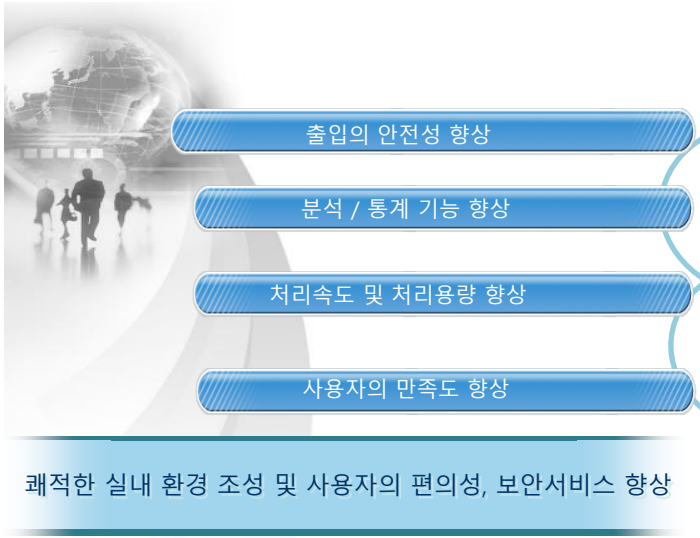
등급	선정 기준
통제구역	인가 받은 자 이외의 불필요한 인원의 출입이 금지되는 구역으로 보안상 비 인가자의 불필요한 접근을 방지하기 위하여 출입자에게 안내가 요구 되는 구역을 말함 외부인의 무단 출입 감시 및 테러 차량의 무단 돌진방지 및 차단을 위한 보안 장치 운영 (차량 돌진 방지 Bollard, 외곽 IR 센서 및 카메라 적용)
제한구역	중요시설 및 자산 등을 보호하기 위하여 보안상 비 인가자의 불필요한 접근을 방지하기 위하여 출입자에게 안내가 요구 되는 구역을 말합니다. 빌딩 내 외부인 무단 출입 차단 장치 운영(로비 보안 Speed Gate, 사무실 RF Reader 적용) 위험물 반입 차단을 위한 검색 보안 장치 운영 (X-RAY검색장비, 금속탐지기 적용)
제한지역	비밀이나 중요시설, 자산 및 중요증서 등을 보호 하기 위하여 일반 출입자들에 대한 감시가 요구되는 지역을 말합니다. 카드 도용에 의한 출입을 차단을 위해 생체인식 장치 운영 (얼굴 인식 Reader + 지문인식기 적용)

4 출입통제 시스템 제안사항

제안사와 고객사의 동상이몽

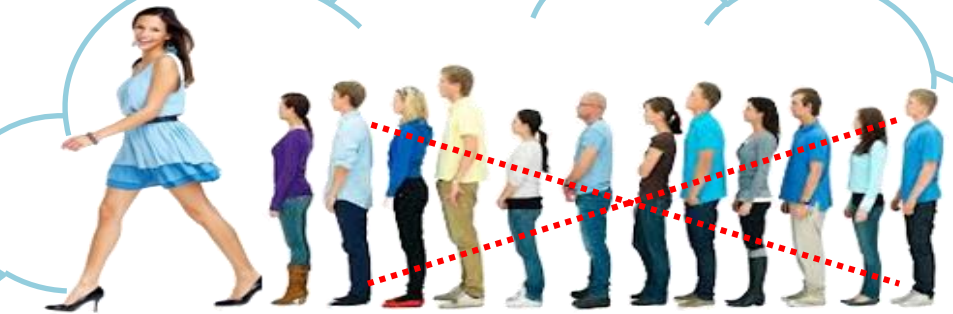
"저희가 설계해드리는 시스템은 이런면이 편리하고, 이런부분이 강화되어있고 … 안전합니다." - 제안 담당자-

"이것도 되고 저것도 되고 … 이런것도 되고 … 안전하고 편리하고 비용이 저렴하면 좋겠어요" - 고객사 보안 담당자 -



- 출입의 안전성 향상
- 분석 / 통계 기능 향상
- 처리속도 및 처리용량 향상
- 사용자의 만족도 향상

쾌적한 실내 환경 조성 및 사용자의 편의성, 보안서비스 향상



적절한 타협으로 올바른 설계를 해야 합니다.

4 출입통제 시스템 제안사항

“출입통제 도입한 10개 기업 중 7곳, 보안사고 대응 계획 없어”

00일보 2017.12.15보도

정부청사 출입보안 사고 美사례 벤치마킹

00일보 2016.05.04 보도

ACESS CONTROL UNIT

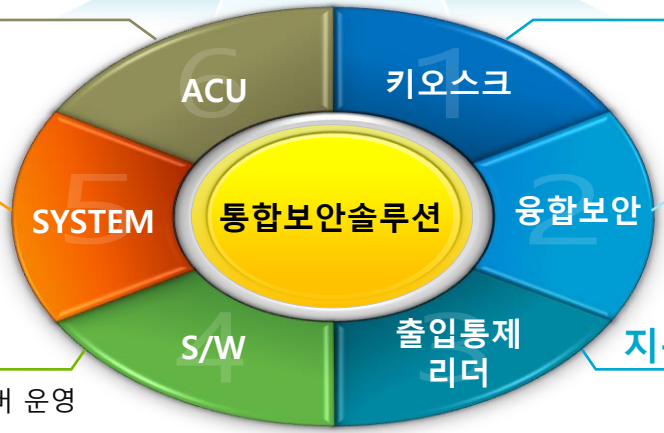
- 종합 중계 기능 수행
- 하위 장치에 대한 감시
- 운영의 안정성 확보

안전한 시스템 운영

- 정전 및 화재 대비
- 통신단절 시 운영

출입통제 SOFTWARE

- Workstation 운영 / Client 서버 운영
- 기존의 시스템간 통합 연동
- 종합적 시스템 관리 및 제어
- 사용자관리, 시스템관리, Alarm Monitoring



자동화 시스템 운영

- 내용 확인 등
- 정보검색
- 안내시스템

융합보안서비스

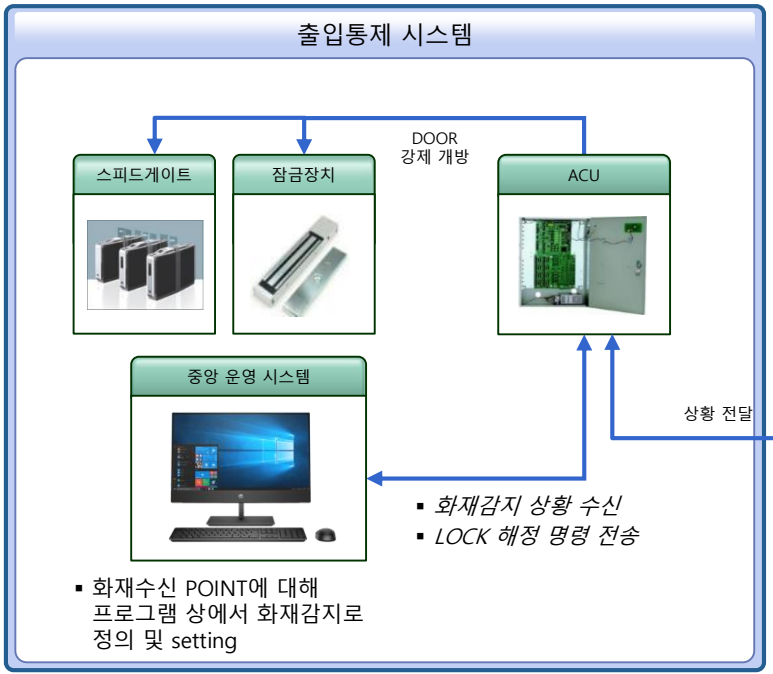
- 물리적 보안강화
- 정보보안강화

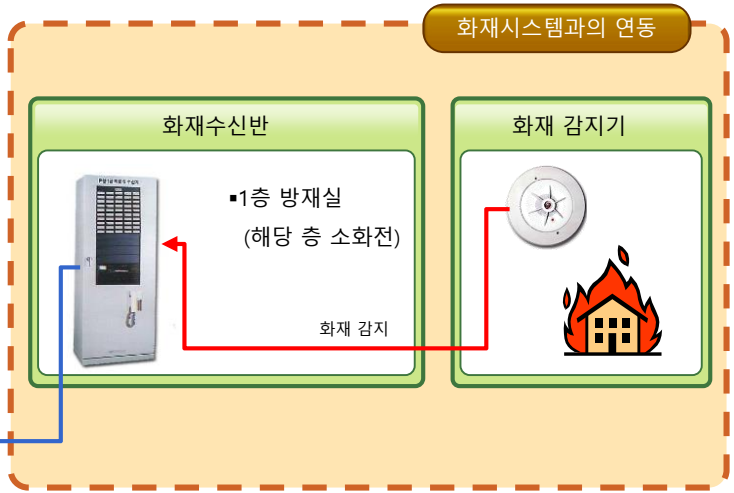
지문/카드리더 등 단말장치

- 초고속 알고리즘
- 신뢰성 있는 동작
- 강력한 내구성 확보
- 진피인증의 정확성

4 출입통제 시스템 제안사항

화재 등의 비상 상황 발생시 내부 근무자의 탈출 및 소방인력의 건물내부 출입이 용이하도록 화재 수신반과 연동하여 모든 출입문은 자동으로 열리도록 구성합니다. 또한 재실 현황을 확인 할 수 있어야 합니다.



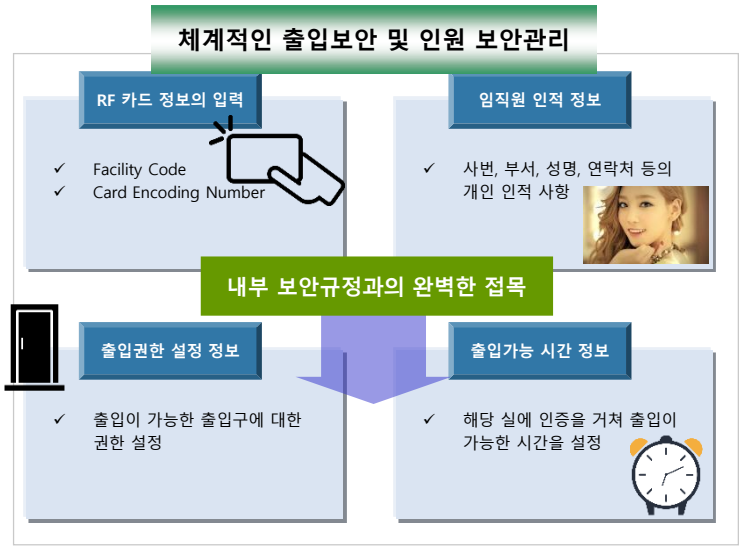


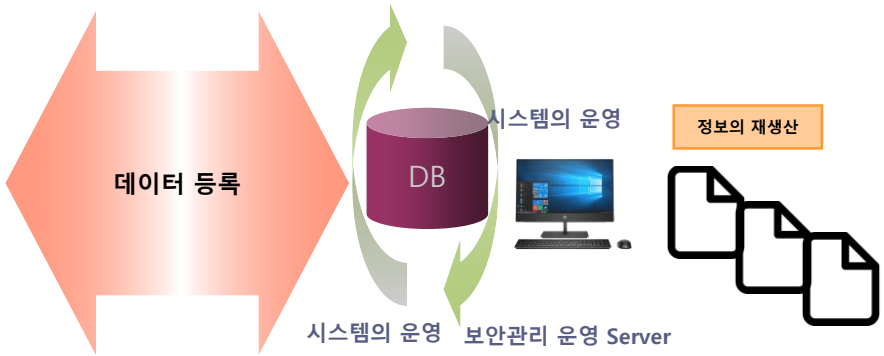
소방방재 시스템 (화재수신반)과 연동시켜 화재발생시 모든출입문과 스피드게이트, Lock을 즉시 개방하여, 내실자들이 화재에 빠르게 대처할 수 있게 합니다.

또한 시스템 운영 서버에 화재 사실이 즉시 표시되어 보다 효율적인 방재 관리를 하도록 구축합니다.

4 출입통제 시스템 제안사항

안정된 시스템 설계



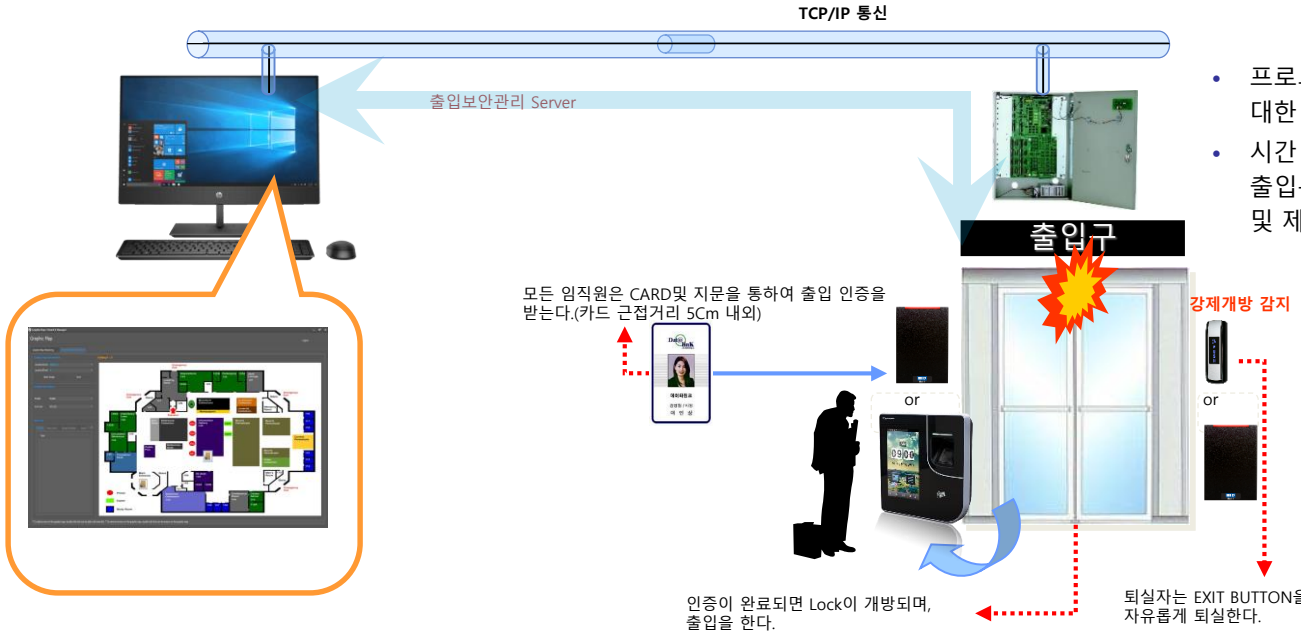


출입통제시스템은 통합보안관리 운영 Server를 통하여 제반 하위 장치들이 종합적이고 체계적으로 관리 운영되며 운영 프로그램 상에 등록된 인적 정보와 물적 정보들은 보안관리 규정에 입각해 운영이 가능하도록 구축된다. 이러한 체계적인 관련 정보들은 시스템 운영을 통하여 정확한 출입정보로 재생산 된다.

4 출입통제 시스템 제안사항

안정된 시스템 설계

출입 및 불법 침입과 관련된 모든 상황은 중앙 감시실로 전송되며 기록이 저장.



- 프로그램 상 선택되어진 출입문에 대한 원격 개방 및 폐쇄
- 시간 제어(Time Schedule)에 의한 출입문 개방 및 폐쇄, 운영 모드 변경 및 제어(지문, 카드, 비밀번호)

4 출입통제 시스템 제안사항

안정된 시스템 설계

사용자 기초 분석

소프트웨어 구성 현황분석,
사용자의 편리함 추구

서비스 설계

기존 보유, 데이터 연계
및 품질관리, 프로세스 설계
효율적 운영을 위한 설계

서비스 설계/구축에 대한
최적화된 사업형성

서비스 계획수립

안정적 시스템 활용 계획 수립
기존 장비와 신규 장비의
융합 활용 계획 수립
시스템 효율적 운영 계획 수립

시스템 구축

기존 장비 연계.제공.관리 시스템 개발

4 출입통제 시스템 제안사항

사업 경험 노하우 및 체계적인 사업 수행

01

- 기초 현황 분석 결과를 기반으로 특화 서비스 개발 및 구성 전략을 제시
- 개발 및 솔루션 정보에 대한 활용 방안을 수립
- 시스템의 확장성 및 고도화 계획을 수렴한 인프라 활용 계획을 수립
- 지원기관 및 지자체에서 보유하고 있는 정책, 홍보, 지원사업을 분석하고 자원의 관리체계와 서비스 제공 방안을 수립

유사 사업으로 검증 된 개발 기술 보유

02

- 전문인력과 핵심 보유 역량을 이용한 플랫폼 설계 및 개발
- 시스템 연계의 이용 활용도 및 신기술의 효율성 향상을 위한 기술 보유
- 유사 사업으로 통합관리시스템 등 요구사항에 따른 개발 제공
- 체계적이고 다양한 구색을 구성하여 개발 제공

서비스 퀄리티 확보를 위한 전문 협력 업체 투입

03

- 변화에 유연하게 대처할 수 있고 고유의 아이덴티티를 유지할 수 있는 강력한 솔루션을 구축
- 다양한 구축 경험을 바탕으로 유사한 성격을 갖고 있는 출입통제서비스를 분석하고 이를 통해 서비스의 아이덴티티 정립 및 보안의 극대화를 구현

4 출입통제 시스템 제안사항

경쟁사들의 제품을 비교하여 설계

경쟁사 비교

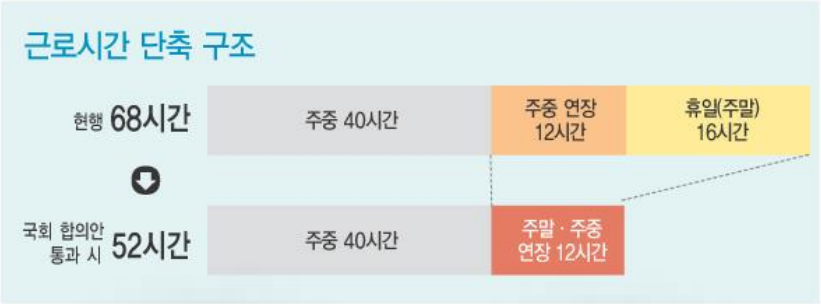
항목		케이제이테크	슈XXX	유XX
지문 인식	FAR (타인인식 오류 률)	< 0.00001 %	-	< 0.0001 %
	FRR (인식거부 오류 률)	< 0.01 %	< 0.1%	< 0.1 %
	1:N 인식 지원	Y	Y	Y
	1:N 인식 속도	2,000 지문 시: 0.1 초 30,000 지문 시: 0.5 초	1,200 지문 시: 0.97 초	- (0.8초~)
	센서방식	광학식 500 DPI	광학식 500 DPI	광학식 500 DPI
	CPU	32bit CPU	DSP 400 MHz	ARM9
사용자 ID	사용자 ID	1-99999999	-	-
	사용자 용량 (지문 탬플릿)	최대 50,000~100,000 명	최대 50,000 명	최대 50,000
통신방식	RS-485	Y	Y	Y
	TCP/IP	Y	Y	Y
	USB 지원	Y	Y	Y
주요 기능 기타	운영모드	비밀번호/카드/지문/카메라 조합	비밀번호/카드/지문조합	비밀번호/카드/지문조합
	외부 인터페이스	위건드, USB	위건드, USB	위건드, USB
	파워	DC 12 V	DC 12 V	DC 12 V
	이벤트 저장 용량	500,000	500,000	500,000
	기타 (제품특징)	Color LCD 사운드 기능 예비 Relay기능 자체오류 검사 기능 CE, FCC 인증, Wifi지원, BlueTooth지원	Color LCD CE, FCC 인증 등 Wifi지원 고품질 사운드	Fake지문 인식기능 탑재 CE, FCC 인증 등

경쟁사 제품 비교

항목		KJ TECH KJ-3400	유XX AC4000
지문 인식	FAR (타인인식 오류 률)	< 0.00001 %	< 0.0001 %
	FRR (인식거부 오류 률)	< 0.01 %	< 0.1%
	1:N 인식 지원	Y	Y
	1:N 인식 속도	2,000 지문 시: 0.1 초	1,200 지문 시: 0.97 초 -
	센서방식	광학식 500 DPI	광학식 500 DPI
	CPU	32bit CPU	32bit CPU
사용자 ID	사용자 ID	1-99999999	-
Card	지원가능카드	HID, EM,Mifare, IClass,Indala,Felica,Desfire 외	EM, Mifare
통신방식	RS-485	Y	Y
	Tcp/IP	Y	Y
	USB 지원	Y	Y
주요 기능 기타	LCD	Color TFT LCD	흑백LCD
	외부 인터페이스	위건드, USB	위건드, USB
	파워	DC 12 V	DC 12 V
	기타 (제품특징)	Color LCD / 사운드 기능 예비 Relay기능 / 자체오류 검사 기능 / CE, FCC 인증	

4 출입통제 시스템 제안사항

사회적 이슈가 되면 솔루션으로 설계



- 서울지방고용노동청 시행
- 고객 맞춤형 근로형태 맞춤 서비스
- Variety / Non Actions / Management / Real Time

Variety

다양한 Communication 채널을 통해 사업장에 최적화된 솔루션을 제공

Non Actions

직원들의 Action 없이도 사업장내 들어오면 출근, 퇴근,외출 등의 관리를 자동으로 체크

Management

사업장마다 근태정책이 다를 경우 각 사업장마다 관리할 수 있는 기능 제공

Real Time

관리자가 실시간으로 출, 퇴근레포트 및 실시간 모니터링 기능 및 스케줄러 기능 가능

4 출입통제 시스템 제안사항

사회적 이슈가 되면 솔루션으로 설계

방문예약 등록, 권한 설정

- 방문예약 신청
- 예약현황 확인
- 방문내역 확인

데이터 처리 방안

- 엑셀 저장
- 상세 검색
- 보고서 저장
- 등록정보 및 통계 보고서 인쇄

로그인 관리

- 일반 임직원 권한 화면
- 안내데스크(경비실) 권한 화면
- 관리자 권한 화면

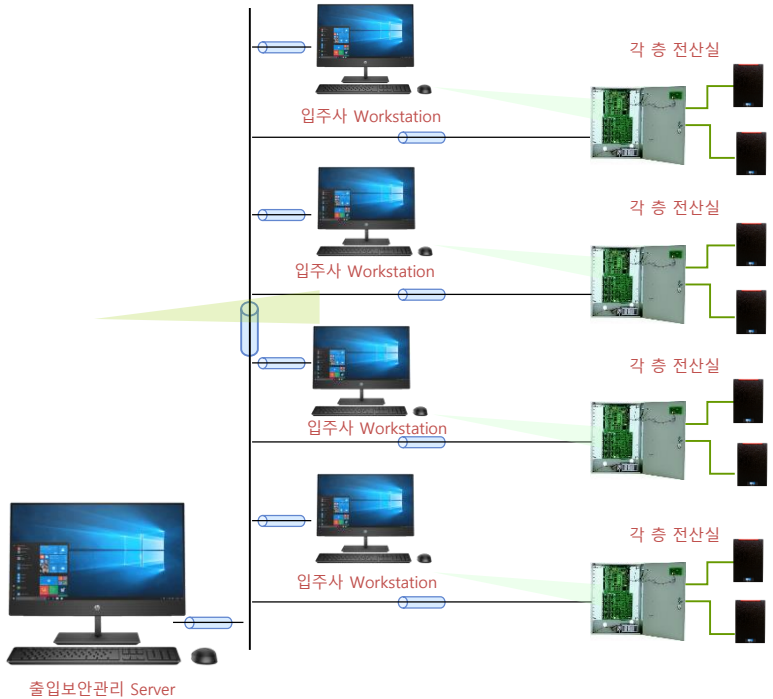
병동 면회객 관리 시스템 기대 효과

병동 출입 관리시스템 도입으로 한국형 병문안 문화 개선
2차 감염 발생율 최소화로 시민이 안심하고 방문하는 진료환경 조성
감염병 발생 시 실시간 방문객 통제 및 관리 기반 마련
신속하고 효율적인 2차 감염 경로 파악 기반 확보
사용자 편의 중심의 연계 프로세스 설계로 업무 효율성 증대
방문객 통제에 따른 의료진 업무 효율성 향상 및 기관 신뢰도 향상
체계적이고 통합적인 보안 관리를 통해 무결성 확보

감염 통제 및 방문객 편익을 위한 병원 환경에 적합한 출입통제시스템과 출입자 인증 및 권한 설정을 위한 센서 기반의 접촉 / 비접촉식 시스템 설계 및 구축.
병원 면회객실 운영서비스 연계를 고려한 시스템 구축 / ICT기술을 활용하여 원내감염을 최소화 할 수 있는 출입관리솔루션을 구축

4 출입통제 시스템 제안사항

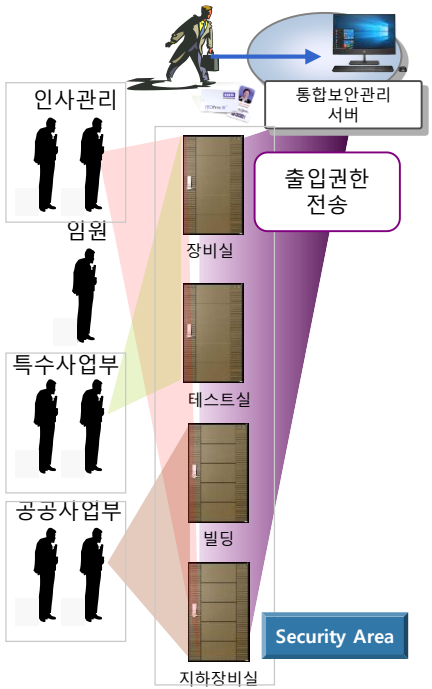
운영의 시스템화



- ✓ 통합보안관리 서버는 모든 시스템을 통합 제어 및 관리 한다.
- ✓ 통합보안서버로 부터 적절한 권한을 부여 받은 Workstation은 지정된 층의 출입구에 대해서만 모니터링 및 관리가 가능하다.
- ✓ 보안관리 통합서버의 마스터는 입주사 직원에 대해서 해당 층과 정문 출입구, 메인로비, 엘리베이터 홀만 출입이 가능하도록 출입권한을 부여할 수 있고, 각 사무실 출입은 제한한다.

4 출입통제 시스템 제안사항

운영의 시스템화



■ 보안 등급 운영(*예. 자체 내규에 의거 적용)

보안 1등급(개인/그룹)

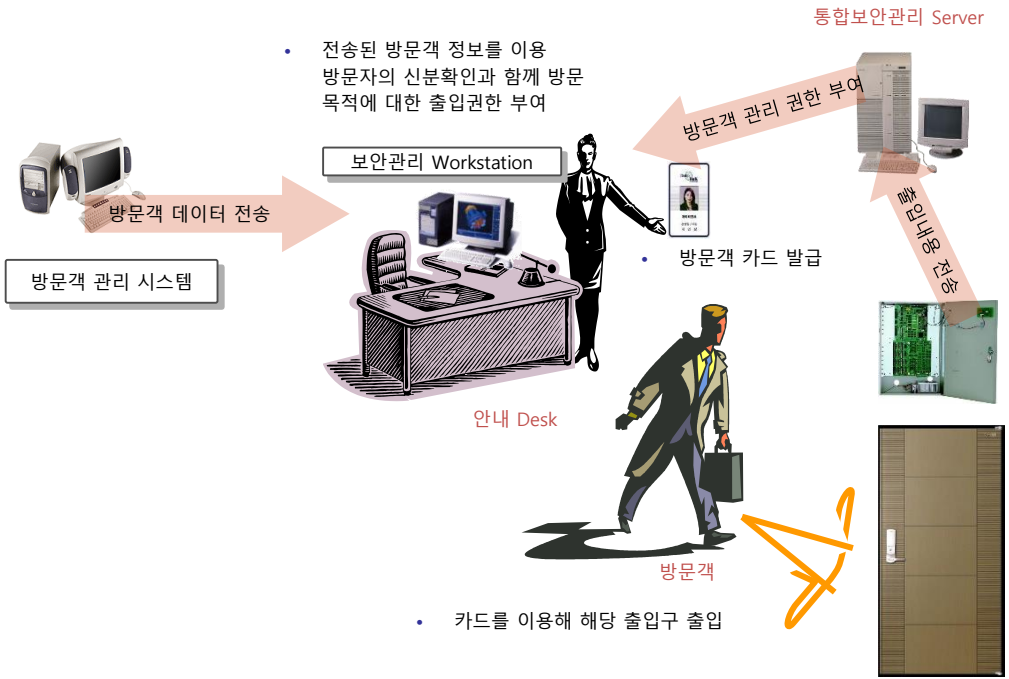
보안 2등급(개인/그룹)

보안 3등급(개인/그룹)

- 보안 1등급 : 내부 모든 출입문에 대한 출입
- 보안 2등급 : 각종 특수 실 제한
- 보안 3등급 : 일반 사무실 만 출입

4 출입통제 시스템 제안사항

운영의 시스템화

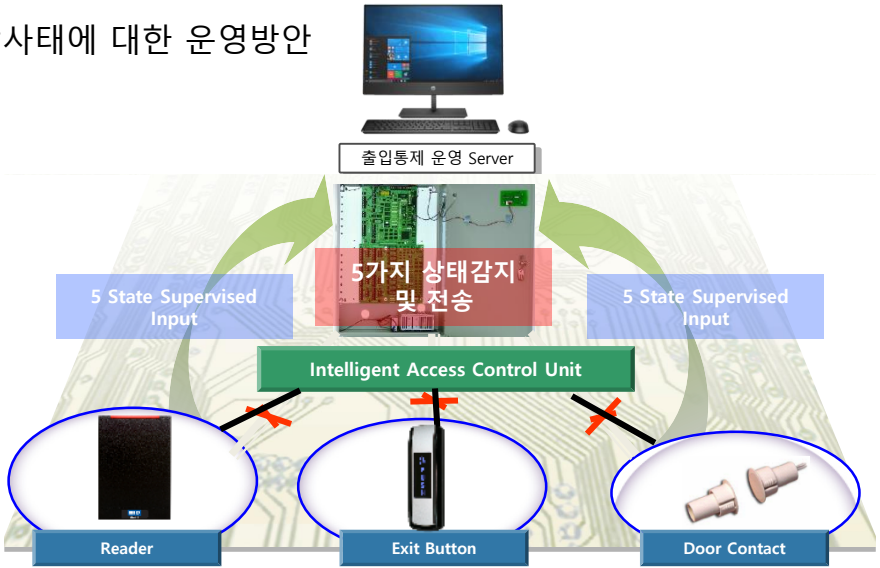


- ✓ 방문자는 최초 기 구축된 방문객 관리 시스템에 접속하여 관련된 방문사항을 입력하며, 입력된 방문자 정보는 안내 Desk에 설치된 보안관리 Workstation에 전송된다.
- ✓ 방문객 전용 카드는 공통 출입구(메인로비, 1층 엘리베이터홀)에 대해서는 사전 출입권한이 부여되며 방문 출입구에 대해서는 안내 Desk관리자에 의해 출입권한이 부여된다.
- ✓ 방문객 출입과 관련된 모든 정보는 통합보안관리 서버에 전송되어 지며, 전송된 방문객 관리정보는 저장 및 레포트로 출력이 가능하다.
- ✓ 설정할 수 있는 카드의 종류는 다음과 같다.
  - ✓ 상주직원, 계약직 및 방문자 등을 구분하여 카드의 유효기간을 설정할 수 있다.
  - ✓ 상주직원카드 (Permanent)
  - ✓ 임시 출입카드 (Temporary)
  - ✓ 방문객 카드 (Visitor)
  - ✓ 제한 기능의 임시 카드 (Temporary with Limited Use)
  - ✓ 제한 기능의 방문자 카드 (Visitor with Limited Use)

4 출입통제 시스템 제안사항

운영의 시스템화

비상사태에 대한 운영방안



ACU의 자기진단

- ACU는 이상상황 발생 시 즉각 자기 진단기능을 수행
- 그 결과를 내장된 LED로 표시
- 운영 프로그램으로 상태 전송

하위 장치들의 상태 감시

- ACU와 연결된 본 하위 장치들은 5가지 상태확인이 가능하도록 운영된다.
- 이상 상황에 대해서 정확한 진단 결과를 운영 Server에 전달함으로써 운영자의 오인을 사전에 방지한다.
- 정확한 결과 인지를 통해 적절한 대처를 할 수 있다.

출입통제를 주 임무로 하는 본 시스템은 사용자에 의해 발생된 상황에 대해서만 운영하는 것이 아니라 시스템에 대한 전반적인 상태감시까지 겸할 수 있도록 운영 된다. 이는 하위 하드웨어 장치들의 정상적인 작동 여부를 파악하고 더 나아가 정확한 이상 내용을 시스템이 자체 진단하고 그 결과를 운영자가 쉽게 인지할 수 있도록 한다.

4 출입통제 시스템 제안사항

운영의 시스템화

불법행위에 대한 경보발령 및 대처 방안

Card Reader

카드판독 장치인 카드리더를 부착된 상태에서 떼어 내었을 시 이는 운영 프로그램으로 통보되며, 이를 출력한다.

ACU

ACU는 Security Area내에 위치 하나 함체를 임의적으로 개방 했을 시 이는 즉시 운영 프로그램으로 통보된다.

Door

Door에는 개폐 및 강제개방을 감지할 수 있는 Door Contact과 상태감지가 가능한 Electric Lock으로 설치된다.
강제개방 시에는 운영 프로그램에서 즉시 경보를 방생한다.

4 출입통제 시스템 제안사항

운영의 시스템화

비상시 운영방안

통신단절 시 운영

정전 시 운영

화재 발생 시 운영

4 출입통제 시스템 제안사항

최첨단 출입통제시스템 구축을 통해 발생 가능한 보안 사고를 사전에 방지하고, 시스템의 효율적 운영 및 감시체제를 확립하며, 비상시 대책 등을 통해 시스템 도입효과를 극대화합니다.

건물 관리 측면

- 국제수준의 보안시설 구축
- 건물의 이미지 개선
- 대외적인 홍보 효과
- 건물의 가치 상승

업무 관리 측면

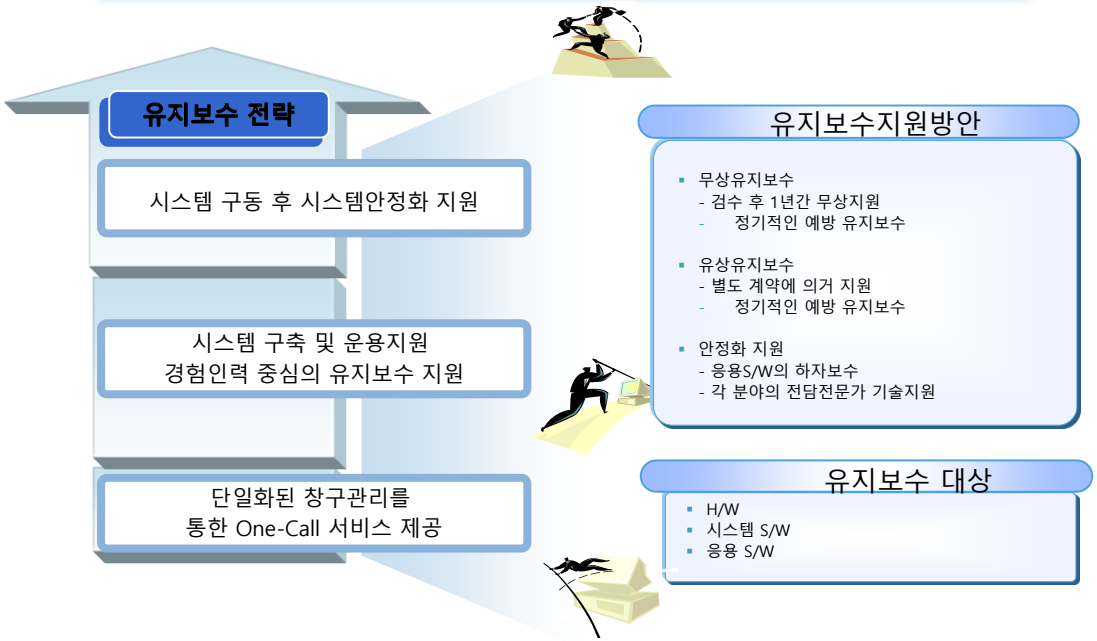
- 기업의 자산 및 정보 보호
- 관계자외 출입제한으로 업무효율 증대
- 임직원의 안전 확보

보안운영자 측면

- 운영의 자동화
- 업무의 편의성 제공
- 종합적인 상황 파악
- 신속한 상황 대처

시공 완료 후 시스템의 안정적 운영을 위해 본 시스템을 구성하고 있는 각종 하드웨어/시스템 소프트웨어/응용 소프트웨어 등을 효율적으로 관리할 수 있는 유지보수 체계를 수립합니다. 원활한 운영 및 시스템의 지속적인 발전을 위해 구축 후의 유지보수 방안을 제시하고, 품질보증활동 및 예방정비활동을 통해 고객감동 서비스를 실현합니다.

신속 정확한 유지보수 지원으로 시스템의 안정적 운영



5

유지보수 계획

유지보수 방법

유지보수는 문제발생시 신속한 복구뿐만 아니라 효과적인 예방정비를 통한 문제발생의 근원적인 차단을 목표로 신속한 유지보수 지원체계를 운영합니다. 이에 납품일로부터 1년간의 무상 유지보수 기간을 확보하여 시스템의 지속적인 기술지원, 장애발생시 신속한 복구지원, 예방정비, 업그레이드로 지속적인 성능향상을 도모할 수 있는 체계적인 활동을 수행합니다.

시스템의 안정적 운영

지속적인 정기점검을 통한
문제발생 요소의 근원적 해결

유지보수 전략

- 일관된 지원체계 보장 및 장애 발생 시 비상연락 체계 유지
- 유상 유지보수 사항 발생시 신속한 대응방안 수립

장애발생 시 최단시간 내 복구

제품에 대한 지속적인 업그레이드

지속적인 기술지원

정기적 성능관리

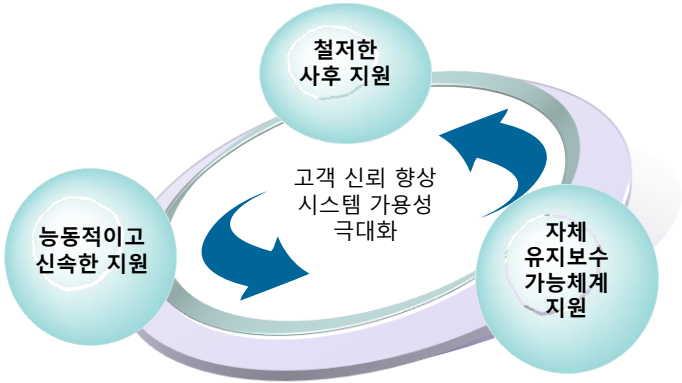
H/W, N/W	S/W, Package	Database
하드웨어 장비 장애 시 유지보수	버전 업그레이드 지원	DB관리 및 데이터 확장

5

유지보수 계획

유지보수 전략

품질보증 활동과 지속적인 예방정비활동을 통하여 문제발생 요소의 근원적인 해결과 신속한 장애처리로 시스템운영의 신뢰향상 및 시스템의 가용성을 극대화하는 것을 유지보수 목표 및 전략으로 설정하였습니다. 이를 구체적으로 정리하면 통합지원체계, 예방 유지보수체계, 상시 지원체계로 요약할 수 있습니다.



5

유지보수 계획

유지보수 원칙

유지보수는 궁극적으로 시스템 관리자 및 운영자를 대상으로 최단 기간 내에 자체 운영 능력과 장애 대처 능력을 확보할 수 있도록 다각적인 차원으로 지원함을 목표로 합니다. 이를 위하여 개발 단계에서는 기술이전 및 교육, 기타 품질보증 활동을 지속적으로 추진하며, 시험 운용 이후부터는 관리자가 자체적으로 시스템 운영관리가 이루어질 수 있도록 전개하는 것을 원칙으로 합니다.

유지 보수 원칙

- 검수 확인일로부터 12개월간 서비스 무상 원격 유지보수 지원
- 장애발생 시 빠른 시간 내에 시스템 정상가동 원칙
- 유지보수 기간 Hardware, Software수정, O/S 업그레이드, 신규 개발 및 변경 보급 시 적극 지원
- 공급 및 개발한 전 시스템을 유지보수 활동에 포함시키고 장애발생 시 신속히 처리
- H/W, S/W 설정 변경 및 최적화 지원
- Network, Database management system 등의 환경변화에 따른 시스템 변경 최적화 지원
- 무상 유지보수기간 만료 후에는 별도의 유지보수 계획에 의하여 지원
- 시스템 운영 및 유지보수가 용이하도록 사용자 지침서(매뉴얼) 작성 및 제공

5 유지보수 계획

유지보수
내용 및 범위

유지보수는 궁극적으로 시스템 관리자 및 운영자를 대상으로 최단 기간 내에 자체 운영 능력과 장애 대처 능력을 확보할 수 있도록 다각적인 차원으로 지원함을 목표로 합니다. 이를 위하여 개발 단계에서는 기술이전 및 교육, 기타 품질보증 활동을 지속적으로 추진하며, 시험 운용 이후부터는 고객사 자체적으로 시스템 운영관리가 이루어질 수 있도록 전개하는 것을 원칙으로 합니다. 개발 단계별 역할은 다음과 같습니다.

Key Point 무상 유지보수

응용 소프트웨어 하자보수	▪ 기능 및 사용자 인터페이스 오류 장애 접수 시 수정 및 복구 ▪ 사용자 관리 지원 ▪ 하자 보완사항에 대한 운영자 및 사용자 교육	납품일로부터 1년
하드웨어 하자보수	▪ 데이터베이스 운영관리 및 활용지원과 운영교육 ▪ 데이터입력 상태 점검 및 백업 및 복구	납품일로부터 1년

KJ TECH의 장애 복구 활동

고객지원 부서의 정기적 예방점검

응용시스템 변경관리

DB 전문가 지원

Key Point 유상 유지보수

유상 유지보수 기본 지침

- 유상 유지보수는 무상 유지보수 기간의 만료 전 계약에 의해 실행
- 기능 추가 및 확장에 관한 시스템 개발은 유지보수 차원이 아닌 시스템 재개발에 관한 협의에 따라 별도의 계획을 수립하여 실시
- 기술 업그레이드는 그 사안에 따라서 대상 및 시기를 주관기관과 협의 하에 결정
- 데이터베이스구축의 추가 작업은 유지보수의 차원이 아닌 주관기관과 협의하여 별도의 계획을 수립하여 계약하여 시행한다
- 재 개발비 산정 시에는 직접 인건비에 재개발 정도에 따라 상호 협의하여 재 개발율, 경비 및 기술료를 바탕으로 산정

유상 유지보수 범위 및 기간

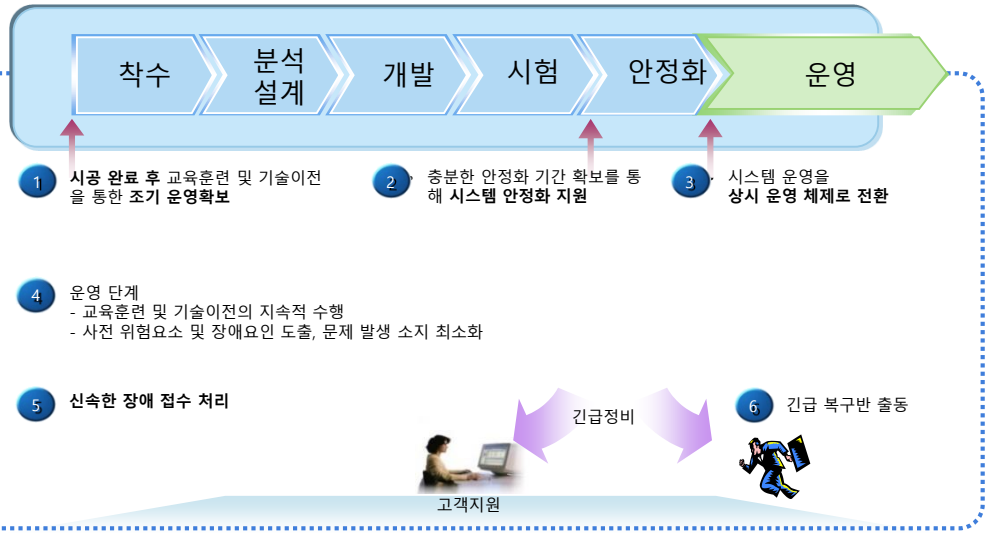
분 야	지 원 범 위	기간
응용 소프트웨어	▪ 사용자 업무생성 및 제도변경으로 인한 프로그램 신규개발 및 수정 ▪ 시스템 기능의 추가확장 ▪ DB 및 시스템 구조의 변경을 요하는 프로그램 수정사항 ▪ 시스템 소프트웨어의 추가설치 ▪ 시스템 소프트웨어 업그레이드(커스터마이징) ▪ 시스템 소프트웨어의 라이센스 추가	추후협의 후 결정
데이터베이스	▪ 데이터베이스 성능 업그레이드	추후협의 후 결정

※ 유상 유지보수 범위에 대해서는 유상 유지보수 계약' 체결시 계약서에 명문화 함

5 유지보수 계획

유지보수 지원체계

유지보수 지원체계는 프로젝트 전반에 걸쳐 시스템 운영관리 및 응용시스템 확장 기능에 대한 기술이전 및 교육을 실시, 프로젝트 착수 시부터 조기 운영요원을 확보하고 시스템의 안정화를 위해 충분한 시험 운영 기간을 통해 품질 및 안정성을 보장하며, 완료 후에는 고객사의 인수인계를 통해 상시 운영체계로 전환하는 체계를 유지합니다.



유지보수 전략

- 신속한 장애처리
- 일관된 지원체계 보장
- 품질보증활동 및 예방정비활동으로 무장애 시스템 지원
- 유상 유지보수 사항 발생 시 신속한 대응
- H/W, S/W 검토 시 필요한 자료의 제공 및 지원


Thank you