콘텐츠 테이블

용어집 1

알파벳 ㄱ ㄴ ㄷ ㄹ ㅁ ㅂ ㅅ ㅇ ㅈ ㅊ ㅋ ㅌ ㅍ ㅎ

용어집

- 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.
- ACID 특성: 데이터베이스에 대하여 원자성(Atomic), 일관성(Consistent), 고립성(Isolated), 영속성(Durable)을 가져야하는 트랜잭션의 특성. 원자성은 더 이상 분류할 수 없는 작업 단위로써 트랜잭션 내에 모든 단계에서 모두 성공하거나 실패해야 하는 특성. 일관성은 데이터베이스를 하나의 안정된 상태에서 다른 안정된 상태로 가져가야 하는 특성. 고립성은 임의의 트랜잭션이 동시에 실행되는 다른 트랜잭션에 영향을 주어서는 안 되는 특성. 영속성은 데이터베이스의 무결성을 유지하기 위해 재구성될 수 있도록 로그를 드라이브에 유지해야 하는 특성.
- Ad Hoc 네트워크: 기지국이나 엑세스 포인트와 같은 네트워크 기반 구조에 의존하지 않고 각각의 장치들에 의해 자율적으로 구성되는 네트워크. 각 장치들은 무선 인터페이스로 통신하지만, 라우팅 기능으로 무선 통신의 거리상 제약을 극복하며, 각 장치들의 이동이 자유롭기 때문에 동적이고 자율적인 네트워크 토폴로지가 형성된다.
- 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.
- FastCGI: 웹 서버 응용 프로그램 언어인 공통 게이트웨이 인터페이스(CGI)에서 하나의 프로세스가 다중 CGI 요청을 처리하도록 하여 속도를 향상시킨 웹 서버 플러그 인 프로그램.
- HF 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.
- IK 등급: 물리적 충격에 대한 제품 보호 정도를 규정한 국제 등급.
- 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.
- JSON: JavaScript Object Notation의 줄임말. 복잡한 객체들의 관계를 문자, 괄호, 기호만으로 표현할 수 있으며, PHP, C#, Python 등 많은 언어에서 사용할 수 있다.
- 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.
- LF 카드: 120~140 kHz 대역을 사용하는 낮은 주파수의 전자식 카드.
- 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(Network Video Record): 네트워크 상에 설치된 카메라나 비디오 장비를 이용해 해당 액세스 포인트에 대해 영상을 녹화하거나 모니터링하고, 발생된 이벤트를 관리할 수 있는 기능.
- OSDP(Open Supervised Device Protocol): 리더에서 컨트롤러로의 단방향 통신만 가능했던 Wiegand 인터페이스를 보완하여 개발된 RS-485 표준 프로토콜. 리더와 컨트롤러 간 양방향 통신 환경에서 대규모 데이터를 처리할 수 있으며, 바이오메트릭 데이터의 전송 또한 가능하다. 이 프로토콜을 지원할 경우 타사 장치간 연결도 가능하기 때문에 기존에 구성되어 있는 시스템에서 교체가 필요한 항목만 바꿔 사용할 수 있다.
- PoE(Power over Ethernet): 이더넷 케이블을 통해 장치에 전원을 공급하는 시스템. 하나의 케이블을 이용해 장치에 데이터를 전송하고 전원을 공급할 수 있기 때문에 설치와 확장이 간편하며, 배선 비용을 절감할 수 있다.
- REST (Representational State Transfer): 웹과 같은 분산형 시스템을 위한 소프트웨어 아키텍처의 한 형식이다. HTTP URI를 이용하여 정보의 자원을 표현하여, HTTP Method(GET, POST, PUT, DELETE 등)으로 행위를 표현한다.

  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.
- RTE 버튼: Request To Exit의 약자로, 내부에서 출입문을 열기 위한 버튼이다. 이 버튼을 누르면

출입문이 열리며, 퇴실할 때 별도의 인증이 필요하지 않은 출입문이나 구역에 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 프로토콜이며 TCP와 IP를 조합한 것.
- TLS: Transport Layer Security의 줄임말로, 웹 클라이언트와 웹 서버가 네트워크로 통신할 때 보안과 데이터 무결성을 위해 사용하는 암호 규약을 의미한다.
- UHF(Ultra High Frequency): 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.
- 가져오기: 다른 컴퓨터 시스템에서 데이터를 자신의 시스템 내로 읽어오는 것.

  감사 추적: 시스템의 변경 정보를 기록한 정보. 사용자의 허가되지 않은 행위, 사용자 행위의 처리 과정, 등에 대한 정보 조사가 가능하다.
- 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): Advanced Encryption Standard의 줄임말. 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.
- 그래픽 맵: BioStar에서 제공하는 모니터링 방식의 하나로, 도면상에서 출입문의 상태를 실시간으로 확인하고 제어할 수 있는 기능.

- 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.
- 근태: 출근과 결근을 포함하여 직원의 근무 시간에 관한 정보를 수집 및 추적하는 관리 기능.
- 근태 규칙: 직원들이 근무한 시간을 파악하고 관리하기 위해 관리자가 정의한 규칙.
- 근태 이벤트: 직원의 근태 상황을 나타내는 이벤트. 직원들의 출입 시간을 기록하여 특정 기간 동안 근무한 시간을 계산한다.
- 글로벌 구역: 서버와 마스터 장치가 TCP/IP로 연결되고, 마스터 장치와 슬레이브 장치가 RS-485 통신으로 연결되어 통신하는 구역. 해당 구역의 마스터 역할을 서버가 수행한다.
- 급여 시스템: 직원의 근무 시간 및 근태, 기타 세금 등의 요인에 따라 총 임금을 계산하여 정확한 급여를 지급하기 위한 시스템.
- 내보내기: 특별한 형식의 데이터를 사용하는 프로그램이 자신의 데이터를 다른 프로그램이 사용할 수 있는 형태로 저장하는 것.
- 노이즈: 신호를 모호하게 하거나 식별하기 어렵게 만드는 전기적 신호.
- 다이렉트 모드: BioStar 2 클라이언트에서 연결 가능한 장치를 직접 검색하여 연결하는 방식으로, 클라이언트에서 장치 및 서버와의 통신을 담당한다. 서버에서 장치 검색 시 연결 가능한 장치 목록이 나타나며, 관리자는 해당 목록에서 연결할 장치를 선택할 수 있다.
- 다이오드: 전류가 한쪽 방향으로만 흐르도록 제어하는 부품으로, 도어락이 동작할 때 순간적으로 발생하는 역전류를 방지하기 위해 사용한다.
- 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 수행하는 장치.
- 데이지 체인: 데이지 체인이란 연속적으로 연결되어 있는 하드웨어 장치들의 구성을 지칭한다.
- 데이터베이스 관리 시스템 (DBMS): DataBase Management System의 줄임말. 데이터베이스를 조작하는 소프트웨어. 즉, 데이터베이스 관리 시스템이 데이터베이스를 관리하며, 응용 프로그램이나 사용자가 데이터베이스에 접근하여 데이터를 사용할 수 있도록 한다.
- 도어 컨택: 출입문 센서의 다른 말. 출입문의 현재 상태(닫힘/열림)를 확인하기 위한 자기 센서.
- 동기화: 서로 다른 시스템이나 네트워크에서 시간이나 정보 등을 일치시키는데 사용.
- 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.
- 등록: 사용자의 바이오 정보를 바이오 인식 시스템에 저장하기 위한 일련의 절차. 샘플 수집, 템플릿 생성 및 저장 등이 해당한다.
- 로그: 시스템, 네트워크, 장치, 출입문 등에서 발생하는 모든 이벤트의 기록.

- 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. 호스트(Host) 장치라고도 부른다.
- 매칭 타임아웃: 장치 혹은 서버 매칭에 주어지는 제한 시간. 시간 내에 매칭이 완료되지 않을 경우 매칭이 실패된다.
- 맨트랩: 부정 출입을 방지하고 비보안 영역과 보안 영역을 분리하기 위한 물리적 출입통제 시스템.
- 멀티 RFID 카드 기술: 125kHz, 13.56MHz와 같이 서로 다른 대역 주파수의 카드를 하나의 장치에서 읽을 수 있는 기술.
- 메시지 표시 타임아웃: 사용자의 조작이 없을 때 메시지가 화면에 표시되는 시간.
- 모니터링: 특정 목적을 위한 감시 활동. 출입통제 및 근태관리에서 모니터링은 출입통제 및 사용자의 근태 이벤트를 확인하거나 장치 및 출입문, 구역의 상태를 실시간으로 확인하고 제어하는 것을 의미한다.
- 모델 번호: 제조사가 장치 식별을 위해 부여한 고유 번호.
- 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 (인식) 정보: 개인의 신원을 식별할 수 있는 정보. 개인이 가진 고유한 신체적, 행동적 특징을 갖는 정보로 지문, 서명, 정맥 패턴, 얼굴, 음성, 홍채, 유전자 등을 말한다.
- 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 제어 목록에 따라 허용 또는 차단한다.
- 백 라이트: 액정 표시 장치의 가시성을 위해 액정 뒤에서 비추는 조명.
- 백 라이트 타임아웃: 백 라이트가 켜진 뒤 유지되는 시간.
- 병렬 포트: 병렬 인터페이스를 통해 데이터를 동시에 전송하는 방식의 입출력 접속구.
- 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 대칭 키로만 복호화가 가능하다.
- 본인 거부율 (오거부율): FRR(False Rejection Rate). 바이오 인식 시스템의 정확성을 비교하는 데 사용되는 기준으로서 등록자를 비등록자로 인식할 확률.
- 부재 관리: 휴가, 출장, 외출, 외근 등으로 인한 근로자의 부재를 관리하는 것.
- 분기점: 두 개의 지문 융선이 만나거나 나누어지는 지점.
- 블랙리스트: BioStar 장치에서 인증이 거부되는 카드 목록. 카드를 분실하거나 도난당한 경우 블랙리스트에 카드 ID를 등록하여 오용을 방지할 수 있다.
- 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.
- 사용자: 슈프리마 장치를 사용하는 개인.
- 사용자 ID: 특정 사용자를 식별하기 위해 사용되는 영어 또는 숫자로 이루어진 식별 부호.
- 사용자 그룹: 관리의 용이성을 위한 사용자 집합. 출입 그룹의 구성 요소.
- 사용자 동기화: BioStar 서버에서 변경된 사용자 정보를 자동으로 장치에 보내는 것.
- 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.

- 소집 구역: 화재 등 긴급 상황 발생 시 구성원이 모이도록 지정된 구역. 특정 구역에 있는 인원의 수와 명단을 모니터링하거나, 특정 구역에 사용자가 일정 시간 이상 체류하는 경우 알람 및 경보로 관리자에게 알려줄 목적으로 사용한다.
- 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.
- 슈프리마 템플릿: 슈프리마에서 정의한 지문 템플릿.
- 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.
- 스케줄 개방: 특정 구역의 출입문이 미리 정해진 스케줄에 따라 개방되는 기능.
- 스케줄 잠금: 특정 구역의 출입문이 미리 정해진 스케줄에 따라 잠기는 기능.
- 슬레이브 장치: RS-485로 연결한 장치 중 리더 또는 입출력 기능만 수행하는 장치. 사용자 정보를 갖고 있지 않으며 마스터 장치에 의해 제어된다.
- 시간 기록: 근무 시작 또는 마감 시간을 나타내는 이벤트.
- 시간 동기화: 네트워크에서 서로 다른 장치 또는 시스템 간에 시간을 동일하게 맞추는 기능.
- 시간외 근무: 근로기준법 또는 사규에서 정한 1일 근무 시간을 넘어서 근무하는 것으로 조기 출근, 잔업, 휴일 근무 등이 포함될 수 있다.
- 시리얼 통신: 여러 개의 비트를 순차적으로 전송하는 통신 방법. 대표적으로 RS-232와 RS-485가 있다.
- 식사 공제: 일일 총 근무 시간을 계산할 때 식사 시간을 제외하는 것.
- 실시간 로그: 각각의 액세스 포인트에서 실시간으로 발생하는 이벤트에 대한 기록.
- 실시간 비디오 보기: 비디오를 이용한 모니터링 방식의 하나. BioStar에서는 IP 카메라의 화면과 이벤트 로그를 실시간으로 제공하며, 해당 출입문을 수동으로 열거나 잠글 수 있는 기능을 지원합니다.
- 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.
- 알람: 시스템에서 발생한 이벤트 중 실시간으로 조치가 필요한 이벤트 종류.
- 알람 액션: 알람이나 특정 이벤트가 발생하면 자동으로 장치를 제어하거나 이메일 전송 등을 수행.
- 암호: 개인이 사용자 ID와 함께 인증을 위해 사용하는 문자열.
- 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.
- 액세스 온 카드: 사용자의 ID와 크리덴셜, 출입 그룹 정보를 기록한 카드.
- 얼굴 검출: 장치에서 사용자의 크리덴셜을 검증한 뒤 출입을 허가하기 전에 사용자의 얼굴도 함께 촬영하여 해당 이벤트와 얼굴 이미지도 함께 저장하는 기능. 얼굴이 검출되지 않을 경우 인증이 실패된다. 얼굴 이미지가 저장되었을 때 필요에 따라 이벤트 발생 시 기록된 사용자 아이디와 얼굴 이미지를 비교하여 동일인임을 확인할 수 있다.
- 얼굴 인증: 사람의 얼굴 특징을 이용하여 신원을 확인하는 기술 또는 그러한 인증 체계.
- 업그레이드: 하드웨어나 소프트웨어의 성능을 기존 제품보다 뛰어난 새것으로 바꾸는 작업.
- 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.
- 유동 근무: BioStar에서 제공하는 근무 규칙 중 하나로, 출근과 퇴근 시간이 정해져 있지 않으며 사용자가 출근하는 시간에 따라 해당 날짜의 근무 규칙이 적용되는 방식.
- 융선: 지문을 나타내는 하나의 지문 곡선으로서 연속되는 융선과 중간에 끊어지는 끝점, 2개의 융선이 만나는 분기점으로 되어 있으며, 이들을 특징점(minutiae)이라 부른다.
- 음성 안내: 사용 가능한 옵션을 사용자에게 음성으로 안내하는 기능.
- 응용 프로그램 프로그래밍 인터페이스 (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.
- 이벤트: 사용자, 장치, 출입문 간에 발생하는 상호 작용. BioStar 서버에 로그로 기록되며 인증 성공 및 실패, 출입문 상태 변화, 경보, 알람 등이 있다.
- 이중 인증: 제한된 시간 안에 서로 다른 두 사람의 크리덴셜을 순차적으로 입력하는 인증 방식.
- 인증: 사용자가 입력한 크리덴셜을 검증하여 신원을 판별하는 동작.
- 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.
- 일괄 등록: 여러 장의 출입 카드를 BioStar 서버에 등록하는 것을 말하며, 등록된 카드는 개별 사용자에게 할당할 수 있다.
- 일광 절약 시간(DST): 서머 타임(Summer Time)이라고도 하며, 하절기에 낮 시간을 효율적으로 사용하여 에너지를 절약하기 위해 시간을 표준시보다 일정 시간 앞당겨 사용하는 것을 의미한다.
- 입출력 장치: 정보 입출력 기능을 수행하는 장치.

- 잠금 장치: 출입 통제 시스템과 연결되어 출입문을 잠그는 데 사용되는 전차 장치. 출입문에 내장되었거나 장착된 전자 장치를 통칭한다.
- 장시간 문 열림: 출입문이 정해진 시간을 초과하여 열린 채 방치된 상태. 알람을 동작하는 트리거.
- 장치: BioStar에서 제어할 수 있는 출입 통제 장치.
- 장치 ID: BioStar에서 하드웨어 장치를 식별하기 위해 부여된 고유한 숫자.
- 재시작: 장치 작동 중 프로그램 실행에 문제가 발생하여 강제로 전원을 완전히 끈 뒤 다시 켜는 것.
- 저전력 블루투스(BLE): 약 10m 내외의 거리에서 2.4GHz 주파수를 이용해 저전력 저용량 데이터를 송수신할 수 있는 블루투스 기술. 저전력 블루투스 기술은 전력의 소모가 매우 적어 전력 공급이 제한되는 소형 장치에 주로 사용되며, 출입통제 분야에서도 모바일 ID 카드의 형태로 활용되고 있다.
- 적합성 판단 엔진(CDE): 슈프리마의 지문 매칭 알고리즘의 절차 중 하나로, 지문 이미지를 처리하여 지문의 특징점을 추출하기 전에 먼저 올바른 지문 이미지를 획득하였는지를 판단하는 단계.
- 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 입력 타임아웃: 지문 정보 입력 제한 시간.
- 지문 템플릿: 지문 이미지에서 발견되는 융선의 끝점이나 분기점 등 일련의 세밀한 특징점을 모은 지문 정보. 특징점의 위치와 개수를 비교하여 식별에 사용한다.
- 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.

- 출근 기록: 출근 시간을 기록하는 것.
- 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: 출입 통제를 위한 물리적인 장치가 설치되는 곳으로 출입 통제의 기본이 되는 공간적인 개념.
- 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.
- 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 레이아웃: 카드 내 데이터의 배열 및 구조.
- 카드 모드: 카드 소지자를 인증하는 방식으로 카드 ID 모드와 템플릿 온 카드 모드, 2가지 방법이 있다. 카드 ID 모드는 카드에 저장된 카드 ID를 기준으로 장치 내에 저장된 사용자 ID와 지문 정보를 비교하는 반면, 템플릿 온 카드 모드는 사용자가 입력한 지문과 카드 내의 지문 정보가 일치하는지 검사하여 사용자의 신원을 파악한다.
- 카드 일련 번호 (CSN): Card Serial Number의 줄임말. 제조사가 부여한 카드의 고유 번호.
- 카드 판독기: 카드에 저장된 정보를 읽어 컨트롤러로 전송하는 장치.
- 커널: 운영체제의 가장 핵심적인 부분으로서 메모리, 프로세스 등의 중요 자원을 관리하며, 부팅 시 메모리에 로드되어 여러 가지 기본 서비스를 제공한다.
- 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 기준으로서 비등록자를 등록자로 잘못 인식할 확률.
- 트랜잭션: 데이터베이스에 대한 조회나 갱신 조작 등으로 구성되는 처리의 기본 단위. 갱신에 의해 일시적으로 일치하지 않는 데이터가 사용되지 않도록 하기 위해 묶어서 처리한다. 트랜잭션이 충족해야 하는 기술적 요건은 ACID 특성이 있다.

- 탬퍼: 장치 상태를 모니터링할 수 있는 방법의 하나로써 외부 요인에 의해 장치가 설치된 브래킷에서 분리될 경우 경보가 울리거나 서버에 이벤트가 기록되게 설정할 수 있다.
- 테일게이팅: 부정 인증을 이용한 출입 방법의 하나로, 제한된 구역에 대한 출입 권한이 없는 사람이 앞 사람을 따라 진입하는 것. '2인 진입'이라고도 하며, 피키배킹(Piggybacking)과 함께 가장 대표적인 부정 출입 방법에 속한다. 일반적으로 테일게이팅은 의도를 가지지 않은 부정 출입을, 피기배킹은 의도를 가진 부정 출입을 의미한다.
- 템플릿: 바이오 특징을 추출한 후 부호화하여 저장한 데이터로서, 바이오 인식 시스템 또는 장치에서 사용자가 입력한 바이오 샘플과 비교하여 신원을 파악하는 데 사용됨.
- 템플릿 온 카드: 사용자 정보 및 지문 템플릿을 저장할 수 있는 스마트 카드.
- 퇴근 기록: 퇴근 시간을 기록하는 것.
- 퇴실 버튼: 출입문을 열기 위한 버튼. 이 버튼을 누르면 출입문이 열리며, 별도의 인증이 필요하지 않은 출입문이나 구역에 사용할 수 있다.
- 트리거 액션: 알람이나 특정 이벤트가 발생하면 자동으로 장치를 제어하거나 이메일 전송 등을 수행.
- 특징점: 지문을 인식하는 데 사용되는 융선의 세밀한 특징적 요소들.
- 틸팅 브래킷: 각도 조절이 가능한 브래킷. 얼굴 인증 장치 또는 홍채 인식 장치에서 주로 사용한다.
- 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.
- 표준 시간대: 동일한 시간을 사용하는 지리적 구역. 출입 통제를 위해 장치나 BioStar의 시간을 설정할 때 사용할 수 있다.
- 프로토콜: 시스템 또는 단말기 사이에 데이터를 교환하기 위해 사용하는 통신 규칙.
- 피기배킹: 부정 인증을 이용한 출입 방법의 하나로, 제한된 구역에 대한 출입 권한이 없는 사람이 의도적으로 출입 권한을 가진 사람과 함께 진입하는 것. 'Piggybacking' 또는 'Piggyback'이라고도 하며, 테일게이팅과 함께 가장 대표적인 부정 출입 방법에 속한다. 일반적으로 피기배킹은 의도를 가진 부정 출입을, 테일게이팅은 의도를 가지지 않은 부정 출입을 의미한다.
- 항시 통과 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.
- 허용 시간: 근태 규칙에 대한 허용 시간. 예를 들어, 출근 시간을 9시로 설정하고 허용 시간을 10분으로 설정했을 때, 9시부터 9시 10분 사이에 출근할 경우 지각으로 처리되지 않는다.
- 협박 지문: 지문 등록 시 특정 이벤트를 발생시키기 위해 지정된 지문. 해당 지문으로 인증하면 로그에 협박 지문 인증으로 로그가 남고 관리자는 이 로그를 이용하여 별도의 알람 설정이 가능하다.
- 화재 경보 구역: 화재가 발생할 경우 모든 출입문 또는 엘리베이터가 개방되거나 잠기도록 설정한 구역.
- 휴가: 미리 정해진 사유 또는 허가를 받고 근무를 쉬는 것 또는 쉬는 기간.
- 휴식: 근무 시간 중 업무를 잠시 중단하고 쉬는 것. 휴식 시작과 종료 시간 사이의 시간으로 계산한다.

From:
https://kb.supremainc.com/knowledge/ -

Permanent link:
https://kb.supremainc.com/knowledge/doku.php?id=ko:glossary&rev=1690789927

Last update: **2023/07/31 16:52**