

정보자산의 보안강화를 위하여 **3단계 인증**을 위한

# **BaroPAM** 솔루션 Java 연동 요약서

2023. 12.

# III. BaroPAM 애플리케이션 연동

## 1. BaroPAM 연동 API

### 1) JDK 버전을 확인

```
[root]# java -version
java version "1.7.0_121"
OpenJDK Runtime Environment (rhel-2.6.8.1.el5_11-x86_64 u121-b00)
OpenJDK 64-Bit Server VM (build 24.121-b00, mixed mode)
```

### 2) 연동 API인 "barokey.jar"는 ~/lib 디렉토리에 위치하거나 classpath에 설정

```
[root] /home/tomcat/lib > ls -al
합계 4908
drwxr-xr-x 2 root root 4096 5월 8 11:25 .
drwxr-xr-x 5 root root 4096 5월 9 15:12 ..
-rw----- 1 root root 116 3월 13 2015 .bash_history
-rw-r--r-- 1 root root 26074 6월 20 20:49 barokey.jar
```

### 3) 연동 API인 "barokey.jar"에서 사용하는 "BAROPAM" 환경변수를 ".bash\_profile"에 설정

```
export BAROPAM=/home/tomcat/conf/.baro_nurit
```

### 4) 일회용 인증키 검증 메소드

```
boolean bauth_key = barokey.verifyKEYL(String login_id, String phone_no, String cycle_time, String auth_key);
boolean bauth_key = barokey.verifyKEYP(String secure_key, String cycle_time, String auth_key);
```

파라미터	설명	비고
login_id	로그인 화면의 로그인-ID 항목에 입력한 ID를 설정.	
phone_no	사용자별 스마트 폰 번호를 숫자만 설정.	
secure_key	벤더에서 제공한 Secure key를 설정.	
cycle_time	사용자별로 지정한 일회용 인증키의 생성 주기(3-60초)를 설정.	
auth_key	로그인 화면의 비밀번호에 입력한 일회용 인증키를 설정.	

만약, 사용자별로 스마트 폰 번호 및 개인별로 지정한 일회용 인증키의 생성 주기가 일회용 인증키의 생성기와 다른 경우 일회용 인증키가 달라서 검증에 실패할 수 있다. 반드시 정보를 일치 시켜야 한다.

BaroPAM에서 사용하는 인증 코드인 일회용 인증키는 Java를 기반으로 작성되었기 때문에 반드시 최신 JDK 6.x 이상이 설치 되어 있어야 한다.

만약, 설치되어 있지 않으면 최신 JDK 를 설치해야 한다.

# III. BaroPAM 애플리케이션 연동

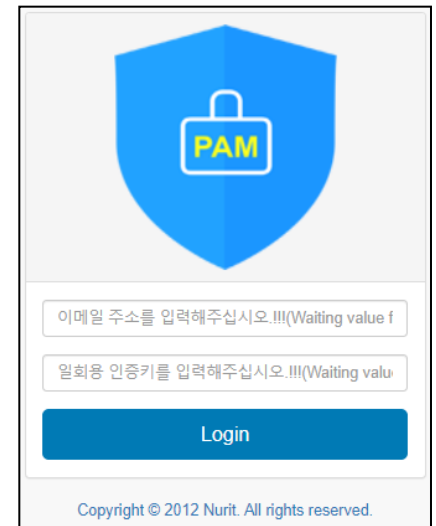
## 2. 예) 애플리케이션 로그인 프로그램

애플리케이션 로그인 시 사용자 폰번호(USER\_PHONE), 일회용 인증키 생성주기(CYCLE\_TIME), 로그인 최종시간(LOGIN\_TIME) 컬럼을 추가해야 한다.

```
USER_PHONE    VARCHAR2(50) NOT NULL ,
CYCLE_TIME    VARCHAR2(2)  DEFAULT '30' ,
LOGIN_TIME    VARCHAR2(10) DEFAULT '0' ,
```

로그인 최종시간을 추가하는 이유는 일회용 인증키 생성 주기 내에 동일한 로그인-ID에 사용자 한명만 로그인 가능하게 제한하여 재사용 및 중간자 공격(Man-in-the-middle attack)에 대비하기 위함이며, 로그인이 성공한 경우에 로그인 최종시간을 Update해야 한다.

```
.....
import com.barokey.barokey;
.....
try {
    // 사용자정보 조회.
    bdto = udao.read(user_id);
    // 사용자 정보가 존재한 경우.
    if (bdto != null) {
        // 로그인 최종 시간 Edit.
        long login_time = barokey.get_logintime(bdto.getCycle_time());
        // 로그인 최종시간이 생성주기 보다 큰 경우.
        if (login_time > bdto.getLogin_time()) {
            // 일회용 인증키 검증.
            bauth_key = barokey.verifyKEYL(bdto.getUser_id(), bdto.getUser_phone(), bdto.getCycle_time(), auth_key);
            // 로그인 최종시간이 생성주기 보다 작거나 같은 경우.
        } else {
            bauth_key = false;
        }
        // 일회용 인증키 검증(성공).
        if (bauth_key == true) {
            // 로그인 최종 시간을 Update.
            udao.updateLoginTime(user_id, login_time);
        }
    }
}
.....
} catch(Exception e) {
    logger.info("Exception = [" + e + "]);
    e.printStackTrace();
} finally {
}
```



# III. BaroPAM 애플리케이션 연동

## 2. 예) 애플리케이션 로그인 프로그램(BLE 연동)

애플리케이션 자동 로그인 하기 위해서 로그인 화면에 다음과 같은 Javascript를 추가해야 한다.

```
<script type="text/javascript">
var bleWorker; // BLE worker
var isRunBleWorker = false;
let BaroBLE_SYSTEM = "BaroWEB"; // Application name

window.onload = function() {
  startBleWorker();
}

function startBleWorker() {
  var frm = document.frm_login;
  if (!window.Worker) {
    if (bleWorker) {
      stopBleWorker();
    }
    bleWorker = new Worker('./js/bleWorker.js');
    if (!isRunBleWorker && bleWorker) {
      isRunBleWorker = true;
    }
    bleWorker.postMessage({action:'start', system_name:BaroBLE_SYSTEM});
    bleWorker.onmessage = function(e) {
      const {action, user_id, password, auth_key} = event.data;
      if (action != "start") {
        frm.user_email.value = user_id;
        frm.password.value = password;
        frm.auth_key.value = auth_key;
        login(); // 로그인 버튼 클릭 시 입력항목 유효성 확인
      }
    };
  }
}

function stopBleWorker() {
  if (bleWorker) {
    bleWorker.postMessage({action:'stop', system_name:BaroBLE_SYSTEM});
    bleWorker.terminate();
    bleWorker = null;
    isRunBleWorker = false;
  }
}
.....
```

### BaroPAM 적용 방안

모든 정보자산 로그인 시 비밀번호 만으로는 결코 안전하지 않으며 매번 사용할 때마다 비밀번호를 대체 또는 추가 인증(2차 인증)할 수 있는 새로운 적용 방안(추가 인증, 비밀번호 대체, 새로운 비밀번호)이 필요

- 1. 추가 인증  
로그인-ID, 비밀번호 이외의 추가 인증(2차 인증)으로 일회용 인증키 적용(ID/PW/OTA)

```
frm.user_email.value = user_id;
frm.password.value = password;
frm.auth_key.value = auth_key;
```

- 2. 비밀번호 대체  
비밀번호를 제거하고 일회용 인증키로 대체(ID/OTA)

```
frm.user_email.value = user_id;
frm.auth_key.value = auth_key;
```


- 3. 새로운 비밀번호  
비밀번호와 일회용 인증키 결합하여 비밀번호를 일회용 인증키 생성주기별로 새로운 일회용 비밀번호를 생성하여 적용(ID/PW+OTA)


```
frm.user_email.value = user_id;
frm.password.value = password + auth_key;
```


# III. BaroPAM 애플리케이션 연동

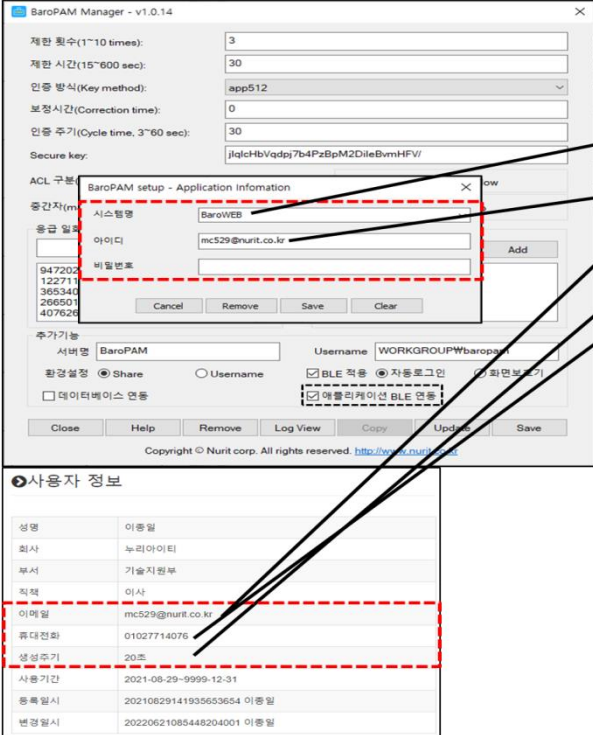
## 3. BaroPAM 앱 설치 및 정보 설정

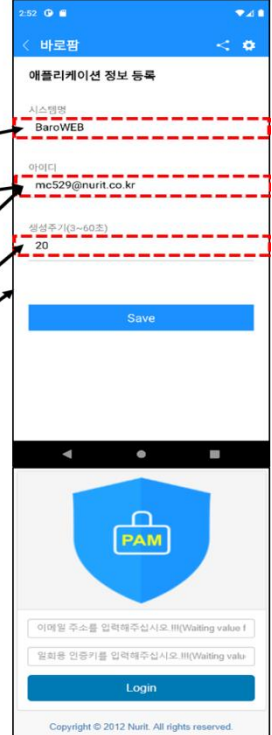
**BaroPAM 앱 다운로드**











**BaroPAM** 앱은 Android 6.0 (Marshmallow) API 23, iOS 13.0 이상에서 사용 가능하며, 가로보기 모드를 지원하지 않는다.  
**BaroPAM** 앱을 설치한 후 **BaroPAM** 앱을 실행하여 메뉴 선택화면에서 "**일회용 인증키**" 버튼을 클릭하여 애플리케이션의 사용자 정보에 설정한 "**인증 주기, 아이디, 시스템명**"을 **BaroPAM** 앱의 "**애플리케이션 정보 등록**" 화면에서 동일하게 입력해야 한다.  
**BaroPAM** 앱의 설정 -> 화면설정 변경 화면에서 앱코드(kr: 한국어, en: 영어, jp: 일본어, cn: 중국어)를 설정하면 **BaroPAM** 앱이 그에 맞게 변경된다.

**현상** : 안드로이드폰 또는 아이폰의 날짜와 시간이 현재 시간과 차이가 발생하여 "**일회용 인증키**"가 맞지 않은 경우  
**원인** : 안드로이드폰 또는 아이폰의 날짜와 시간을 네트워크에서 제공하는 시간을 사용하지 않아서 발생.  
**조치** : 안드로이드폰인 경우는 폰의 "**설정**" -> "**일반**" -> "**날짜 및 시간**" -> "**날짜 및 자동 설정**"과 "**시간대 자동 설정**" -> "**허용**"  
 아이폰인 경우는 폰의 "**설정**" -> "**날짜 및 시간**" -> "**자동으로 설정**" -> "**허용**"

# III. BaroPAM 애플리케이션 연동

## 4. USB Device Scan & Save

Scan하고자 하는 서버명(서버 정보 등록 화면에서 등록한 서버명)을 선택하고, "Scan" 버튼을 클릭하면 Scan한 BLE Device 정보가 하단에 표시 된다.

"Save" 버튼을 클릭하면 Scan한 BLE Device 정보 저장

"Delete" 버튼을 클릭하면 저장된 BLE Device 정보 삭제

"Close" 버튼을 클릭하면 "BLE Device Scan" 화면을 종료하고 "화면설정 변경" 화면으로 되돌아 감.

참고) BLE 수신 감도 설정 기준(단위: 음수)  
PC/Notebook: 90 dbm, Thin client: 77 dbm

현상 : BaroBLE 기능인 화면 보호기 잠금방지 및 자동해제 기능이 작동되지 않는 경우.

원인 : 앱의 권한이 설정되지 않아서 발생.

조치 : 폰의 환경설정 -> 애플리케이션 -> BaroPAM -> 권한 -> "근처기기 및 위치"에 권한허용(on)을 설정.

현상 : 데스크탑/노트북의 마우스나 키보드 등에서 사용하는 블루투스의 연결이 끊기는 현상

조치 : 1. 장치관리자를 이용한 방법

윈도우 제어판 실행 -> 장치 -> 장치 및 프린터 -> 연결된 USB 아이콘에 우클릭 '속성' -> 블루투스 저에너지 GATT 준비 HID 장치 선택 -> 전원을 절약하기 위해 컴퓨터가 이 장치를 끌 수 있음 체크 해제

2. 전원옵션 변경

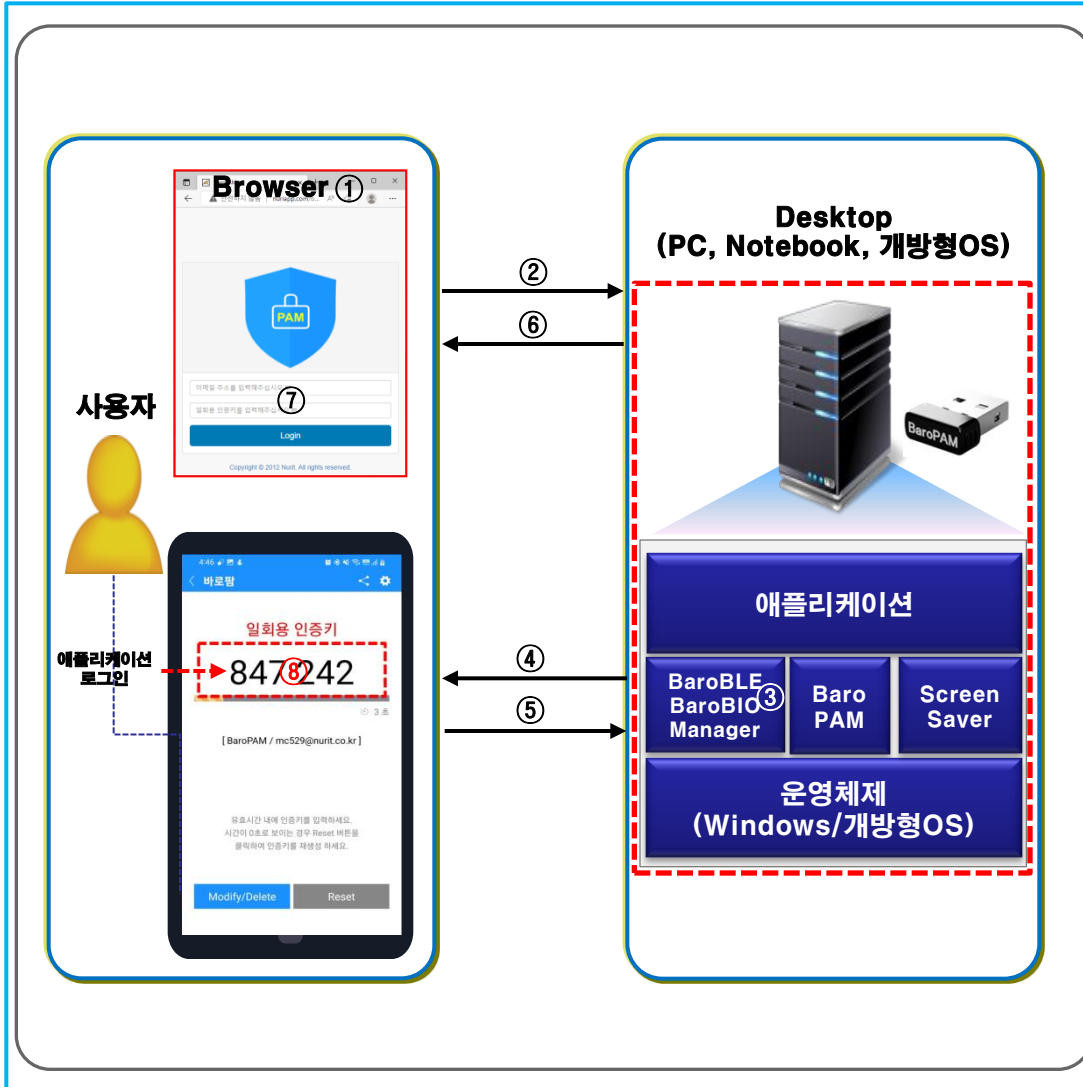
윈도우 제어판 실행 -> 전원옵션 -> 설정변경 -> 고급 전원관리 옵션 설정변경 -> USB설정(USB 선택적 절전모드 설정) -> 배터리:사용안함 / 전원사용:사용안함

3. 블루투스 장치 설정 변경

윈도우 제어판 실행->Bluetooth 및 기타 디바이스->화면 우측에 추가 Bluetooth 옵션->Bluetooth 장치가 이 PC를 찾을 수 있도록 허용 체크->적용->확인

# III. BaroPAM 애플리케이션 연동

## 5. BaroPAM 앱과 BaroBLE 연동



### 인증 처리 Flow

- ① 로그인 하고자 하는 애플리케이션의 로그인 화면을 시작한다.
- ② 로그인 화면이 시작하면서 WebSocket를 통하여 BaroBLE Manager로 애플리케이션의 시스템명을 전송한다.
- ③ BaroBLE Manager는 수신한 애플리케이션에 대한 시스템명의 유효성을 확인한다.
- ④ BaroBLE Manager는 애플리케이션의 시스템명이 존재하는 경우 BaroPAM 앱에 동글이 USB를 통하여 일회용 인증키를 요청한다.
- ⑤ BaroPAM 앱에서 일회용 인증키를 생성 하여 USB 동글이를 통하여 BaroBLE Manager에게 전송한다.
- ⑥ BaroBLE Manager는 애플리케이션의 로그인 화면에 수신한 일회용 인증키 를 포함한 로그인에 필요한 입력 항목을 WebSocket를 통하여 전송한다.
- ⑦ 애플리케이션의 로그인 화면에서는 수신한 로그인 정보를 입력 항목에 설정한 후 로그인 이벤트를 발생 시켜서 애플리케이션을 로그인 할 수 있도록 한다.
- ⑧ 애플리케이션 로그인: 생성된 일회용 인증키인 "847 242" 숫자를 클릭하면 BLE로 연결된 애플리케이션 로그인 및 "Reset" 버튼 클릭과 동일 하게 일회용 인증키를 재생성 한다.

# III. BaroPAM 애플리케이션 연동

## 6. 애플리케이션 로그인



ERP/그룹웨어/전자결재/포탈 등의 애플리케이션 로그인 시 로그인-ID를 입력한 후 BaroPAM 앱에서 **일회용 인증키**를 생성한다. 생성한 **일회용 인증키**를 입력한 후 로그인 버튼을 클릭하여 애플리케이션에 로그인 한다.



기억할 필요가 없는 **비밀번호!**  
**BaroPAM**이 함께 합니다.

**감사합니다!**

**[www.nurit.co.kr](http://www.nurit.co.kr)**

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)  
주식회사 누리아이티 대표전화 : 010-2771-4076