

# 개인정보 유·노출예방

믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다  
Privacy by Trust, Trust by Privacy



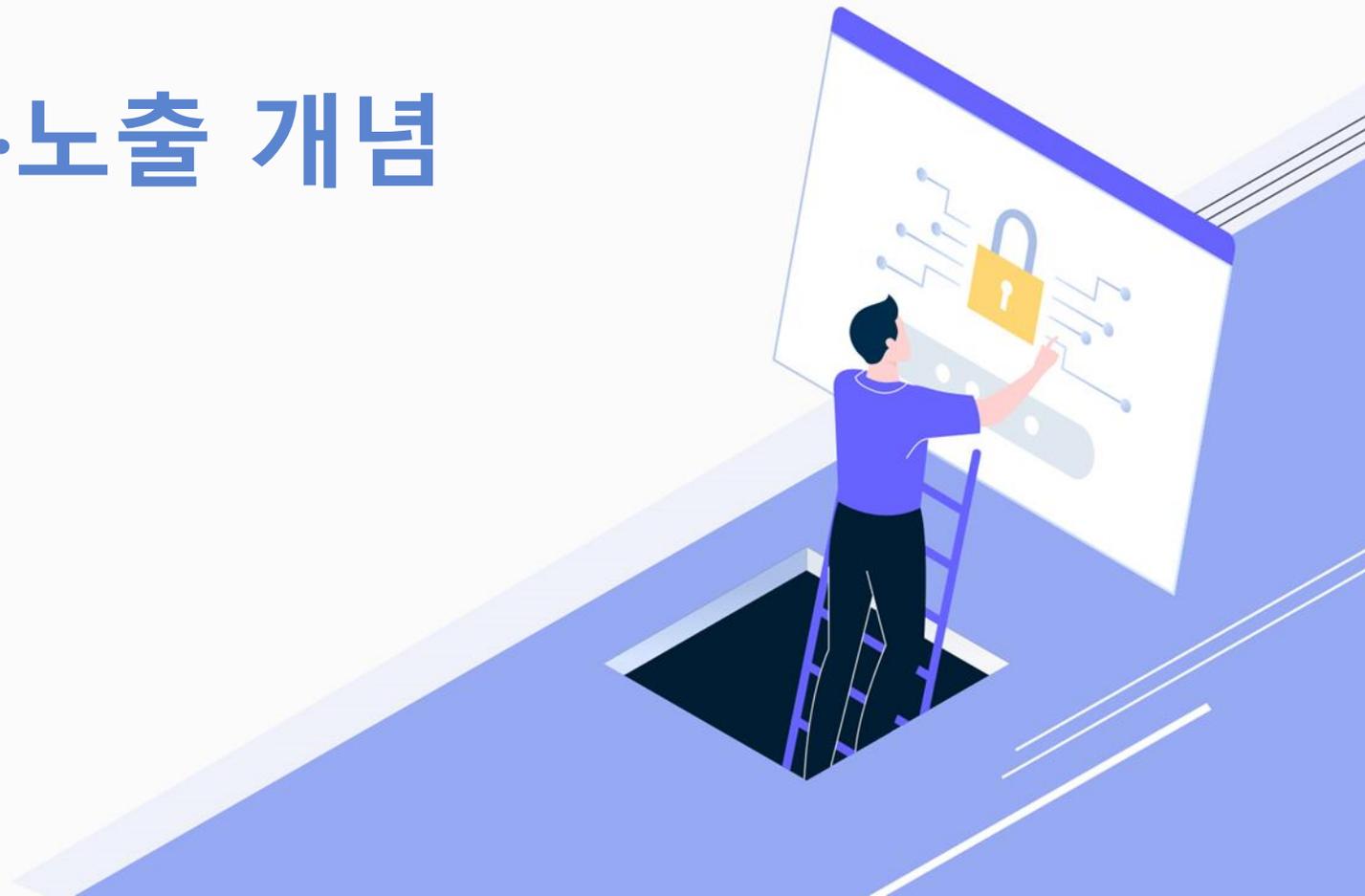
# Contents

- 1 개인정보 유·노출 개념
- 2 개인정보 유·노출 원인 및 사례
- 3 개인정보 유·노출 예방



1

# 개인정보 유·노출 개념





## 1. 개인정보 유·노출 개념

### 🔒 개인정보 “유출” 및 “노출”의 정의

#### ▶ “개인정보” 『유출』이란?

- 정보주체의 “개인정보”에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 경우

#### ▶ “개인정보” 『노출』이란?

- 홈페이지 상 개인정보가 공개되어 누구든지 알아볼 수 있는 상태

#### 유출

- 개인정보가 저장된 DB 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
- 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일, 문서, 저장매체 등이 잘못 전달된 경우
- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난을 당한 경우

#### 노출

- 개인정보가 포함된 게시물이 누구든지 알아볼 수 있는 상태로 등록된 경우
- 이용자 문의 댓글에 개인정보가 공개되어 노출이 된 경우
- 개인정보가 포함된 첨부파일을 홈페이지 상에 게시한 경우



## 1. 개인정보 유·노출 개념

### 🔒 개인정보 노출 모니터링의 중요성

#### ▶ 고유식별정보 등 사생활 침해가 우려되는 정보가 노출

- 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호), 신용카드번호, 계좌번호, 바이오정보 등이 노출

- 주민등록번호는 본인의 동의가 있더라도 법적 근거가 없으면 **처리 불가**
- 바이오정보 등은 처리 시 **본인의 동의 필요** 및 **암호화 보관**하여야 하는 **중요 정보**

#### ▶ 개인정보취급자

- 홈페이지에 노출된 개인정보를 신속히 삭제하지 않을 경우, 제3자에 의해 개인정보가 유출되는 등 급격히 피해가 확산됨

- 개인은 명의도용, 보이스피싱 등 범죄에 악용되고, 대량 스팸 수신 등 피해가 발생
- 기관은 개인정보 유출에 따른 **민사·행정·사법 책임** 및 **이미지 실추** 등





## 1. 개인정보 유·노출 개념

### 🔒 개인정보 유·노출 시 조치사항

#### 노출

- 신속히 노출 페이지 삭제 또는 비공개 처리
- 검색엔진에 노출된 개인정보 삭제 요청 및 로봇 배제 규칙 적용(외부 검색엔진의 접근 차단)
- 시스템의 계정, 로그 등을 점검 후 분석결과에 따른 접속 경로 차단(제3자 접근 여부 파악)
- 재발방지를 위해 서버, PC 등 정보처리시스템의 백신을 최신으로 업데이트 후 디렉토리 점검



#### 유출

- 유출된 정보주체에게 지체 없이 통지(5일 이내)  
※ 정보통신서비스 제공자 등의 경우 "24시간 이내"
  - 유출된 개인정보의 항목
  - 유출된 시점과 그 경위
  - 피해 최소화를 위한 정보주체의 조치방법
  - 기관의 대응조치 및 피해구제 절차
  - 피해 신고 접수 부서 및 연락처
- 피해 최소화를 위한 대책 마련 및 필요한 조치 실시
- 1천명 이상의 개인정보가 유출된 경우
  - 정보통신서비스 제공자 등의 경우 "1건 이상"
  - 국가(개인정보보호위원회 또는 한국인터넷진흥원)에 신고하고 개인정보 유출 사실을 홈페이지에 7일 이상 게재
  - ※ 유출신고: 개인정보보호 종합포털(www.privacygokr) 등



## 1. 개인정보 유·노출 개념

### 🔒 개인정보 유·노출 후속조치

#### ▶ 노출 기관에 대한 조치

- ✓ 개인정보가 노출된 기관에 삭제 등 조치하도록 즉시 통보(이메일, 전화 등)
- ✓ 노출 정부·공공기관 대상 '개인정보 노출 모니터링 결과 통보 및 재발방지 협조 요청' 공문 발송(매월)
- ✓ 노출 기관 담당자 대상 "개인정보 노출 재발방지" 교육 실시(필수)
  - 권역별 집합 교육 참석 요청 공문 발송



반복·대량 노출 기관 및 교육 미참석 기관의 경우,  
"개인정보 관리실태 특별점검" 대상에 포함 가능



## 1. 개인정보 유·노출 개념

### 🔒 개인정보 유·노출 후속조치

#### ▶ 개인정보 처리 기관의 안전조치 의무 및 처벌 규정

##### ✓ 안전조치 의무

- 개인정보 또는 **고유식별정보**가 분실·도난·유출·변조·훼손되지 않도록 안전성 확보에 필요한 **기술적·관리적·물리적 조치** 이행 (개인정보보호법 제24조제3항, 제29조)

##### ✓ 안전성 확보 조치

- 안전성 확보조치에 필요한 세부사항은 인정보보호위원회가 정하여 고시

번호	소명요청	조치할 사항	비고
1	고시 제6조 제3항	취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 <b>접근 통제</b> 등에 관한 조치 시행	
2	고시 제6조 제4항	인터넷 홈페이지를 통해 고유식별정보가 유출, 변조, 훼손되지 않도록 연 1회 이상 <b>취약점을 점검</b> 하고 필요한 보완조치 시행	
3	고시 제7조 제1항	고유식별정보, 바이오정보, 비밀번호를 송신 또는 전달하는 경우 <b>암호화</b>	
4	고시 제7조 제2항	비밀번호 및 바이오정보를 저장 시 <b>암호화</b> (단, 비밀번호는 일방향 처리)	
5	고시 제7조 제3항	인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우 <b>암호화</b>	

※ 정보통신서비스 제공자등의 경우 '개인정보의 기술적·관리적 보호조치 기준' 참조



## 1. 개인정보 유·노출 개념

### 🔒 개인정보 유·노출 후속조치

#### ▶ 개인정보 처리 기관의 안전조치 의무 및 처벌 규정

##### ✓ 처벌 규정

관련 조항	내용	처벌규정
개인정보보호법 제75조 제2항 제6호	✓ 안전성 확보조치 위반	위반 시 3천만원 이하의 과태료
개인정보보호법 제73조 제1호	✓ 안전성 확보조치 미이행으로 개인정보 유출 등 발생 시	위반 시 2년 이하의 징역 또는 2천만원 이하의 벌금

2

## 개인정보 유·노출 사례 및 조치





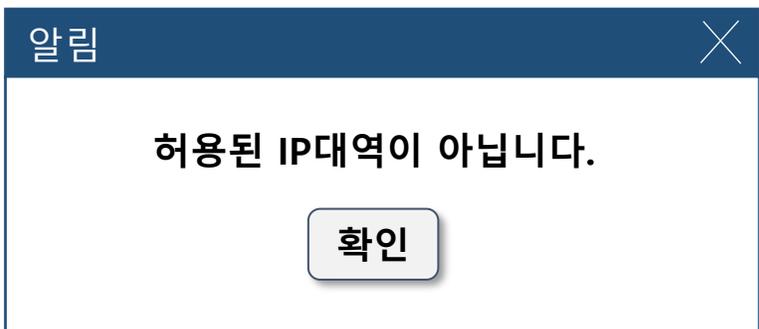
## 2. 개인정보 유·노출 사례 및 조치

### 외부공격

#### DB 관리자페이지 공격으로 인한 유출

##### ✓ 조치

- **Step 1.** 접속권한을 **IP주소, 포트, MAC주소 등으로 제한**하여 인가 받지 않은 접근을 제한
- **Step 2.** 정보통신망을 통해 외부에서 시스템에 접속 시 가상사설망(VPN) 등 **안전한 접속수단**을 사용하거나 **안전한 인증수단**을 적용
- **Step 3.** 개인정보취급자의 계정 설정 시 **안전한 비밀번호** 사용(영문, 특수문자, 숫자로 최소 8자리 이상)
  - \* 특히 DB에 접속하는 DB관리자의 비밀번호는 변경 주기를 짧게 하는 등 강화된 안전조치를 적용
  - \* ID: root, PW: root와 같이 취약한 비밀번호는 사용하지 않음



ID	KISABOAN001
PW	.....



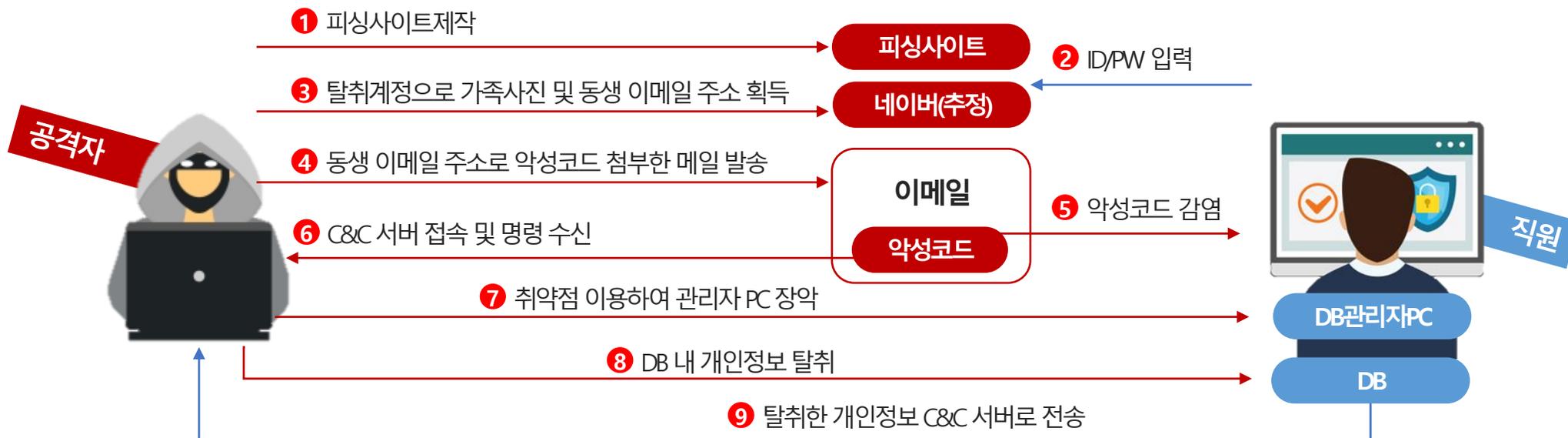
## 2. 개인정보 유·노출 사례 및 조치

### 외부공격

#### ▶ 지능형지속공격(APT, Advanced Persistent Threat)

##### ✓ 조치

- Step 1. **APT공격 대응 솔루션** 도입운영 및 스팸메일과 첨부파일 필터링 및 차단
- Step 2. 의심스러운 이메일 열람 및 이메일 내 **링크 주소 클릭, 첨부파일 실행 등 금지**
- Step 3. **정기 보안교육**과 모의훈련을 통해 취급자의인식 강화





## 2. 개인정보 유·노출 사례 및 조치

### 🔒 고의(내부직원 유출)

#### ▶ 업무 담당자가 지인의 부탁을 받고 고객정보 유출

##### ✓ 조치

- Step 1. 개인정보취급자 교육을 통해 유출사고에 대한 인식 강화
- Step 2. 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여
- Step 3. 내부관리계획에 개인정보 다운로드 기준을 마련하고, 접속기록을 매월 점검하여 개인정보 다운로드 시 그 사유를 확인
- Step 4. 보조저장매체의 반출입 통제를 위한 보안대책 마련하여 비인가된 사용 통제



개인정보취급자  
교육



보안 USB



시건장치가 있는  
케비닛



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 고의(내부직원 유출)

#### ▶ 퇴사한 직원이 개인정보처리시스템에서 개인정보 유출

##### ✓ 조치

- **Step 1.** 개인정보취급자의 계정을 공유하여 사용하지 말고, **취급자 별로 계정을 부여**
- **Step 2.** 전보, 퇴직 등 인사이동이 발생하였을 경우 지체없이 **시스템 접근권한을 변경·말소**
- **Step 3.** 퇴직 점검표에 사용자계정 말소 항목을 반영하여 계정 말소 여부에 대해 확인 절차 마련
- **Step 4.** 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 **최소한의 범위**로 차등 부여
- **Step 5.** 내부관리계획에 개인정보 다운로드 기준을 마련하고, **접속기록을 매월 점검**하여 개인정보 다운로드 시 그 사유를 확인

#### ➔ 개인정보 로그조회

2020.01.01 ~ 2020.03.01 조회

No.	계정	접속 일시	접속지 정보	정보주체	수행업무	상세 보기
1	Admin	2020.01.02 10:23	192.168.1.40	kim134	삭제	
2	Admin	2020.01.25 11:40	192.168.1.40	choi0045	등록	
3	Admin	2020.02.24 13:11	192.168.1.40	lee9204	수정	

#### 개인정보처리시스템 접근제한 관리대장

순번	부서	사용자	계정	업무	접근권한	변경일시	변경사유	처리자
1	인사팀	홍팀장	hong123	인사관리	말소	2020.01.02 10:30	퇴사	Admin
2	인사팀	박대리	pack05	인사관리	인사정보(입력, 조회, 수정, 삭제)	2020.01.25 12:00	입사	Admin
3	인사팀	나직원	najwon33	인사관리	인사정보(입력)	2020.02.24 13:30	부서이동	Admin



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 과실(담당자 업무 관련)

#### ▶ 업무 담당자 행사 안내메일 단체발송

##### ✓ 조치

- Step 1. 외부로 발송하는 이메일의 경우 **개별발송**을 기본 옵션으로 지정
- Step 2. 개인정보취급자 교육을 통해 이름, 이메일 주소가 개인정보임을 숙지
- Step 3. 이메일 개별발송 선택 시 개별발송 여부를 묻는 팝업창 게재 등 **시스템 개선**

받는사람 **kisa@kisa.or.kr** ← 받는 사람에는 노출 되도 문제가 없는 자신의 이메일이나 회사메일 하나정도 넣어주고 나머지 회원들은 숨은 참조에 넣어 개별로 발송

숨은참조 shho...

제목 Gmail에서 숨은참조로 동보메일 발송 방지하기

받는사람  개별발송 ? shh... sy... hr...

참조  개별발송을 위해 체크박스 체크 후 전송

제목  중요 ! 네이버에서 동보메일 발송 방지하기

받는사람 sh... sy... h...

제목 다음에서 동보메일 발송 방지하기

글꼴 10pt 가 가 가 가 가

한명씩 발송  보낸메일 저장  예약 발송

내용입력 후 한명씩 발송 체크 후 전송



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 개인정보가 포함된 게시물 및 댓글 게시

#### ▶ 이용자 문의 댓글에 개인정보 노출

#### ✓ 조치

- **Step 1.** 게시물을 비공개로 전환(게시물 작성자 또는 사이트 관리자)
- **Step 2.** 공개 필요 시, 마스킹 등의 방법을 통해 최소한의 개인정보를 기재
- **Step 3.** 검색엔진에 노출 여부 확인 및 저장된 페이지 삭제

### 홈페이지 관리자의 댓글에 개인정보 노출

작성자 : 김 [마스킹]      작성일 : 2018.06.29      방문 : 10  
제목 : 외국인 등록번호로 회원가입

안녕하세요.

이번에 교환학생으로 재학중인 외국인 친구가 회원가입을 하려고 하는데, 마이핀, 휴대폰이 없어서 본인확인이 불가능해서 회원가입을 못하고 있습니다.

외국인 등록번호로 회원가입을 할 수 있다고 들었는데 어떻게 해야하나요?  
자세한 사항은 통화로 말씀드리고 싶네요.

관리자님 글 확인하시면 전화중 부탁드립니다.

[다음글] 다음글이 없습니다.  
[이전글] 이전글이 없습니다.

목록    답변    수정    삭제

한줄답변

관리자 (06.29)    전화로 말씀하신 외국인 분의 이름 [마스킹], 외국인등록번호 90[마스킹] [마스킹]가 맞나요? 빠른 시일내에 처리해드리겠습니다.

수정    삭제

»  
비공개  
전환

### 게시판을 비공개 게시판으로 운영

#### 온라인상담

번호	제목	작성일
1132	주책 세금 문의	2018-10-29
1131	일반임대사업자에서 주택임대사업자로 전환할 경우에 대해서...	2018-10-26
1130	대형폐기물	2018-10-26
1129	동일한 내용의 행정소송이 최종 승소할 경우	2018-10-26
1128	건물 용도변경 관련	2018-10-26
1127	사업자신고 확인	2018-10-25

등록



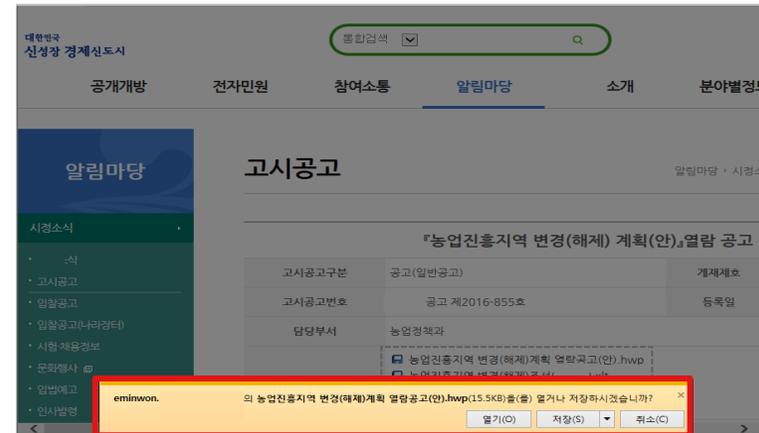
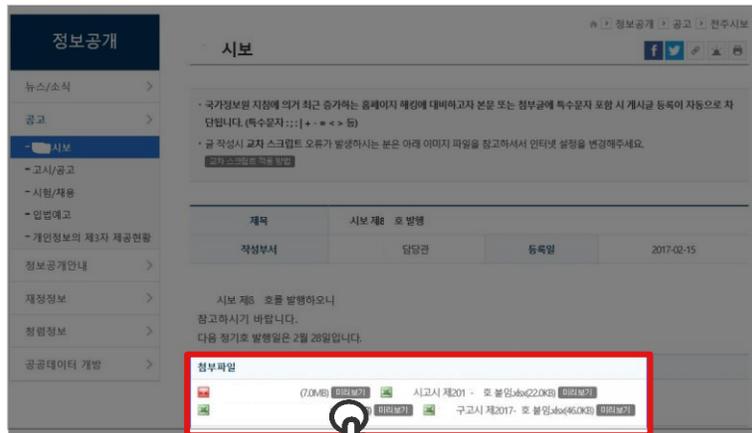
## 2. 개인정보 유·노출 사례 및 조치

### 🔒 개인정보가 포함된 첨부파일 게시

#### ▶ 개인정보가 포함된 파일을 첨부하여 게시판에 게시

##### ✓ 공통 조치

- **Step 1.** 게시물 또는 게시판을 비공개로 전환(게시물 작성자 또는 사이트 관리자)
- **Step 2.** 공개 필요 시, 개인정보 마스킹 등 비식별 처리
- **Step 3.** 검색엔진에 노출여부 확인 및 저장된 페이지 삭제



<클릭 시, "저장" 가능>





## 2. 개인정보 유·노출 사례 및 조치

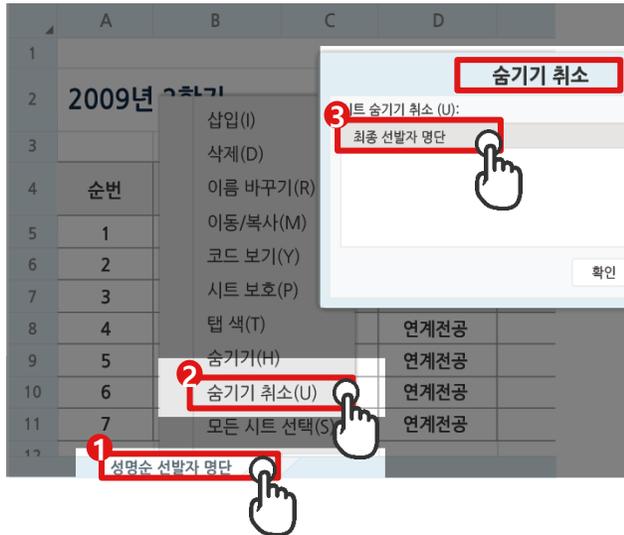
### 🔒 엑셀 파일에 노출

#### ➤ Sheet [숨기기] 처리

##### ✓ 조치

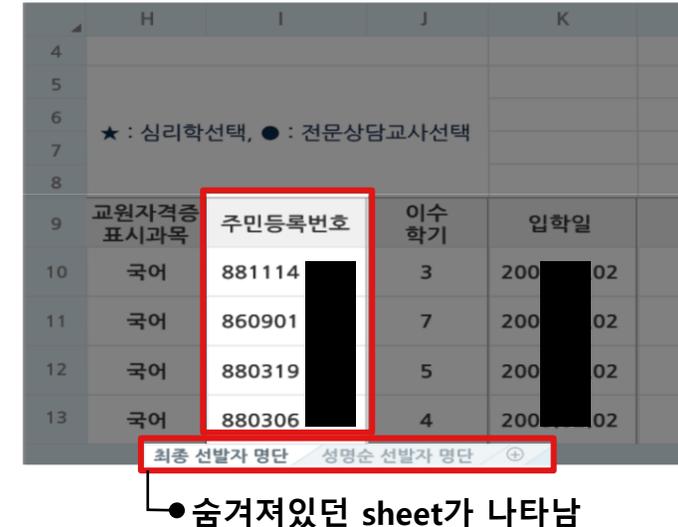
- Step 1. 하단 Sheet 선택 > 오른쪽 마우스 클릭 > 숨기기 취소
- Step 2. 숨겨진 Sheet 삭제

#### Sheet가 숨겨져 있는 파일



»  
숨기기  
취소

#### Sheet 숨기기 취소한 파일



● 숨겨져있던 sheet가 나타남



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 엑셀 파일에 노출

#### ▶ 행/열 [숨기기] 처리

##### ✓ 조치

- Step 1. 열(A,B...) 또는 행(1,2...) 전체선택 > 오른쪽 마우스 클릭 > 숨기기 취소
- Step 2. "행/열"에 기록된 개인정보 삭제 또는 마스킹 처리

#### 행/열 숨기기 처리

B 다음 E ?

A	B	E
대형폐기물스티커 판매 현황		
판매소명	주소	
AA 마트	SS시 AA구 FA동	
BB 타운	SS시 ZZ구 EA동	
NN 마트	SS시 AS구 AS동	
HH 슈퍼	SS시 AW구 SS동	
YY 월물	SS시 AZ구 QE동	
SS 슈퍼	SS시 AX구 EF동	
LL 마트	SS시 BA구 SD동	
AB 동경	SS시 AA구 BB동	
BC 상회	SS시 ZZ구 QQ동	
SF 슈퍼	SS시 AS구 EB동	
CZ 유통	SS시 AW구 CF동	
QW 슈퍼	SS시 AZ구 QB동	
BD 점	SS시 AX구 CV동	
ASE 점	SS시 BA구 BB동	

»  
숨기기  
취소

#### 행/열 숨기기 취소

숨어있던 C와 D가 나타남

A	B	C	D	E
대형폐기물스티커 판매 현황				
판매소명	주소	대표자명	주민등록번호	
AA 마트	SS시 AA구 FA동	조	440227	
BB 타운	SS시 ZZ구 EA동	조	621013	
NN 마트	SS시 AS구 AS동	김	561230	
HH 슈퍼	SS시 AW구 SS동	이	550424	
YY 월물	SS시 AZ구 QE동	이		
SS 슈퍼	SS시 AX구 EF동	조		
LL 마트	SS시 BA구 SD동	유		
AB 동경	SS시 AA구 BB동	남	780822	
BC 상회	SS시 ZZ구 QQ동	김	630417	
SF 슈퍼	SS시 AS구 EB동	이	691110	
CZ 유통	SS시 AW구 CF동	이	750126	
QW 슈퍼	SS시 AZ구 QB동	오		
BD 점	SS시 AX구 CV동	김	750125	
ASE 점	SS시 BA구 BB동	관		



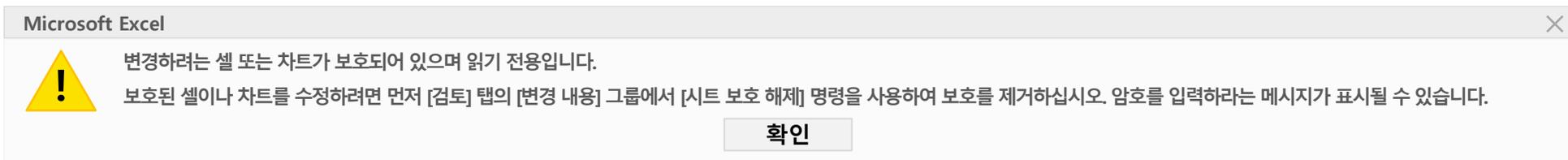
## 2. 개인정보 유·노출 사례 및 조치

### 🔒 엑셀 파일에 노출

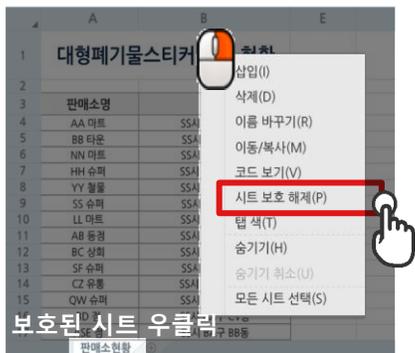
#### ➤ Sheet 보호 처리

##### ✓ 조치

- Step 1. 해당 시트 오른쪽 마우스 클릭 > 시트 보호 해제(P)
- Step 2. "개인정보" 삭제 또는 마스킹 처리

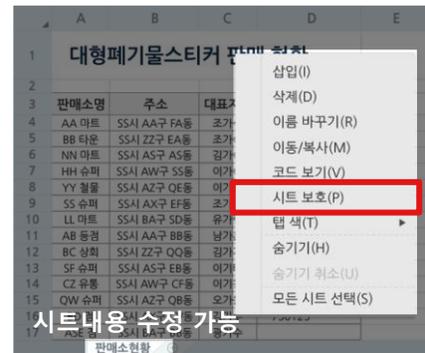


#### Sheet 보호 상태(내용수정 불가)



»  
시트보호  
해제

#### Sheet 보호 해제(내용수정 가능)





## 2. 개인정보 유·노출 사례 및 조치

### 🔒 엑셀 파일에 노출

#### ▶ 외부파일 참조

##### ✓ 조치

- **Step 1.** 엑셀에서 함수 이용 시 셀 안의 값 확인(파일의 경로나 개인정보가 들어가지 않도록 주의)
- **Step 2.** 셀에 값을 넣을 때 데이터의 값만 사용하도록 조치
- **Step 3.** 엑셀 고급 옵션 중 '외부 연결값 저장' 기능 체크박스 해제

#### 외부파일 참조 수식을 이용한 데이터 불러오기

A	B	C	D	E	F	G	H
성명	생년월일	성별	나이	지원구분	최종학력	연락처	주소
홍	199			신	졸	010-12	울시
박	198			경	졸	010-45	중시
이	197			경	졸	010-01	주시
김	196			경	졸	010-52	남시
서	198			신	졸	010-22	광역시
박	199			신	졸	010-82	구시
윤	199			신	졸	010-72	천시
한	199			신	졸	010-52	경시
백	197			경	졸	010-32	울시

»  
함수  
이용 시  
값만 사용

#### 경로 노출 없이 데이터의 값만 이용

A	B	C	D	E	F	G	H
성명	생년월일	성별	나이	지원구분	최종학력	연락처	주소
홍	199			신	졸	010-12	울시
박	198			경	졸	010-45	중시
이	197			경	졸	010-01	주시
김	196			경	졸	010-52	남시
서	198			신	졸	010-22	광역시
박	199			신	졸	010-82	구시
윤	199			신	졸	010-72	천시
한	199			신	졸	010-52	경시
백	197			경	졸	010-32	울시



## 2. 개인정보 유·노출 사례 및 조치

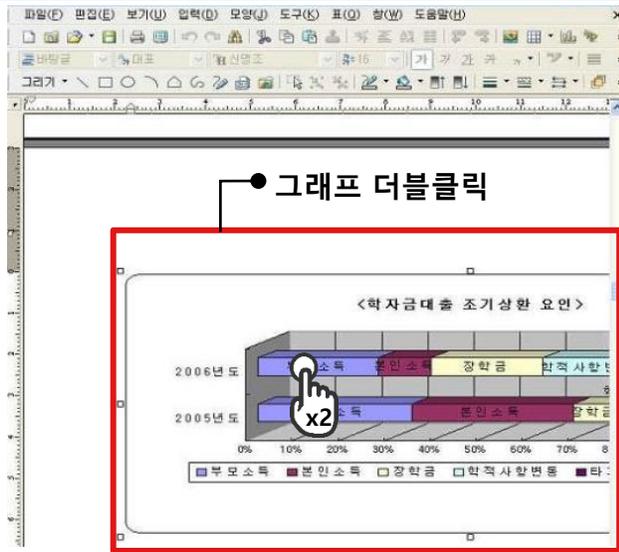
### 🔒 엑셀 파일에 노출

#### ▶ 객체(OLE) 삽입

##### ✓ 조치

- Step 1. 문서 내의 "표" 더블 클릭 후, OLE 객체 내 "개인정보" 포함 여부 확인
- Step 2. OLE 객체(엑셀시트)에 나타난 개인정보 삭제 또는 마스킹 처리

#### OLE 객체가 삽입된 파일



»  
그래프 내  
편집시트  
나타남

#### OLE 객체에 포함되어 있던 엑셀시트

	E1	fx	주민등록번호		
	A	B	D	E	
1	년도	은행	계좌번호	출생년도	주민등록번호
2	2005	민	9452	81	81
3	2005	리	1235	80	80
4	2005	나	2352	49	49
5	2005	협	1324	77	77
6	2005	흥	2646	85	85
7	2005	나	3457	67	67
8	2005	협	9342	55	55
9	2006	리	2232	79	79
10	2006	나	1234	82	82
11	2006	민	5452	46	46
12	2006	리	5652	46	46
13	2006	나	7752	78	78
14	2006	협	9562	81	81
15	2006	흥	1582	67	67
16	2006	나	5342	55	55
17	2006	협	3434	79	79

개인정보  
발견



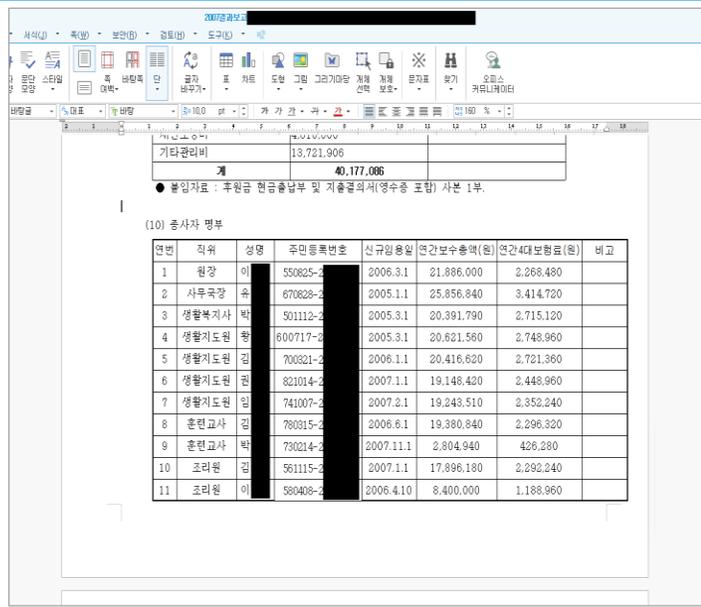
### 🔒 한글파일에 노출

#### ▶ 첨부된 한글파일(HWP, DOC)에 개인정보 노출

#### ✓ 조치

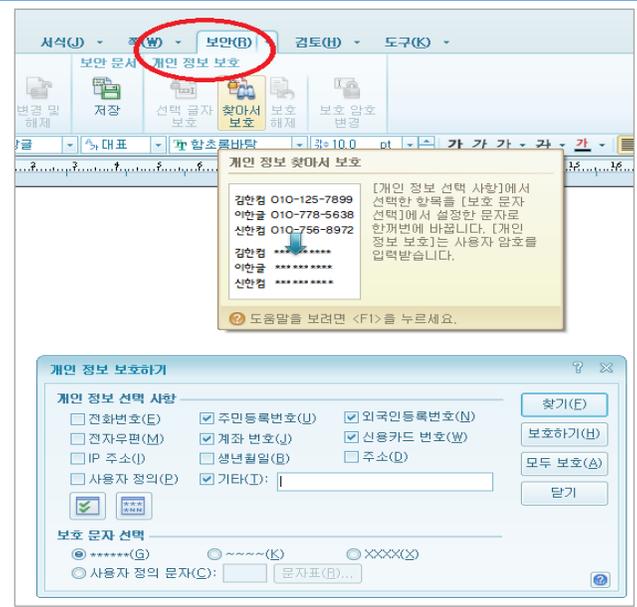
- 문서에 포함된 "개인정보" 삭제 또는 "개인정보 보호" 기능으로 **마스킹**

### 개인정보가 포함된 한글문서



개인정보  
보호기능  
이용

### 한글의 개인정보 보호 기능을 이용





## 2. 개인정보 유·노출 사례 및 조치

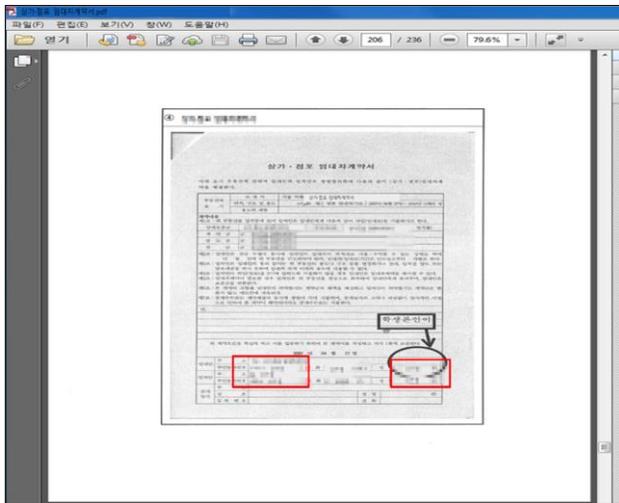
### 🔒 개인정보가 포함된 첨부파일 게시

#### ▶ 이미지 파일(JPG, PDF 등)을 통한 개인정보 노출

#### ✓ 조치

- Step 1. 비공개 게시판 운영
- Step 2. 게시물 비공개로 전환 또는 삭제
- Step 3. 이용자에게 개인정보를 입력하지 않도록 홈페이지 등에 안내

#### 이미지형 PDF 파일에 의한 노출



»  
비공개  
설정

#### 게시판 글 작성 시 안내 문구 삽입 및 비공개 설정

• 표시된 항목은 필수입력 항목입니다.

• 제목

작성자 김

공개여부 비공개 공개

• 내용

첨부파일 ※파일1개당 최대10M까지만 가능합니다.

※ 공개 글 작성 시 주민등록번호, 운전면허번호, 계좌번호 등 개인정보를 입력하시면 안됩니다!

위 글 등록을 위해 가입하신 개인정보수집 및 이용에 동의합니다. (필수)



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 관리자페이지 접근제어 미흡

▶ 관리자만 볼 수 있는 페이지가 인증 과정을 거치지 않고 방치되어 일반 이용자에게 노출

#### ✓ 조치

##### ▪ Step 1. 올바른 관리자 페이지 설정

- ① 관리자 페이지 접속 시 "VPN"이나 "전용망" 등 **안전한 접속수단** 활용
- ② "OTP", "휴대폰", "공인인증서" 등 **안전한 인증수단** 적용
- ③ 관리자 페이지는 **특정 IP 및 인가된 IP**만 접근 가능토록 설정
- ④ 일반 이용자가 접근 가능한 **관리자 페이지 링크 삭제**

- ⑤ 관리자 페이지 주소는 추측하기 어려운 명칭으로 작성
- ⑥ **주기적인** 홈페이지 관리자 비밀번호 변경 및 로그인 시 **안전한 비밀번호 사용**
- ⑦ 미사용 페이지는 즉시 **삭제**

##### ▪ Step 2. 검색엔진에 노출여부 확인 및 저장된 페이지 **삭제**

### 쉽게 유추 가능한 관리자페이지 인증없이 접속



»  
전용망  
구성 및  
VPN인증

### 전용망 사용 또는 인증서비스 적용





## 2. 개인정보 유·노출 사례 및 조치

### 🔒 홈페이지 접속 경로(URL) 관련 오류

#### ▶ 홈페이지 URL 값 변경 시 개인정보 노출

##### ✓ 조치

- **Step 1.** 사용자 자신의 정보만 조회 가능하도록 접근제어
- **Step 2.** 회원 구분 값을 개인정보로 활용하는 경우 변경 필요
- **Step 3.** 홈페이지 설계 변경(GET 방식에서 POST 방식으로) 등을 통해 개인정보 노출 방지

#### URL값 변경 시 다른 회원의 정보가 노출

selectBoardArticle.do?mno=7604

회원정보 수정  
회원의 정보 중 변경된 내용이 있는 경우, 아래에서 수정해주세요.

· 닉네임

· 비밀번호 재설정

· 비밀번호 확인

· 이메일

연락처

학교(학원)지역

학교(학원)구분

»  
파라미터  
방식 변경

#### 파라미터 값이 보이지않게 POST 방식 사용

http://.../mypage/myinfo.php?member\_pno=880924

회원정보 수정

성명

주민등록번호

880924-

http://.../mypage/myinfo.php

회원정보 수정

성명

주민등록번호

880924-



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 홈페이지 소스코드 보안설정 미흡

#### ▶ 홈페이지 설계 오류로 홈페이지 소스코드에 노출

#### ✓ 조치

- Step 1. 인터넷 브라우저의 소스코드 보기 기능을 통해 개인정보가 있는지 확인
- Step 2. 불필요한 개인정보는 소스코드에서 삭제하고 꼭 필요한 정보는 암호화하거나 개인 식별용 구분자를 변경
- Step 3. 검색엔진에 노출여부 확인 및 저장된 페이지 삭제

커뮤니티 > 묻고답하기 > x

커뮤니티! > 묻고답하기

2학기 봉사활동 평가 자원봉사센터.라는 제목을 보고...

이름 : 이 회 조회 : 2643

2학기 봉사활동 평가

라는 제목을 보고 올리는건데.....

자원봉사센터가..안동인가요...???

바로 가기 만들기(M)  
즐거찾기에 추가(F)...  
**소스 보기(V)**  
요소 검사(L)  
인코딩(E)

view-source: **예시**

```
684 <td colspan=2 height=26>&nbsp;&nbsp;&nbsp;이름 : <span_onmousedown="gblayeraction(event, 'gblayer1', 'visible')">
685 <script language="JavaScript">gblayer("gblayer1", "이 회", "tjdgm1857&#064;hanmail.net", "1", "1", "/program
686 <TD onmousemove=msgposit() onmouseover="msgset('2학기 봉사활동 평가', '2006-12-10(일)', '2006-12-10(일)
687 평가');return true;" onmouseout="msghide();window.status='';return true;" width=240><A href="http://www.dovol.ne
688 sin_no=S20060600408&amp;cd_center=young_kyungbuk&amp; jumin_no=931011 &amp;grade=N"><B>2학기 봉사활동 평가</E
689 <TD width=179>
690 <P>자원봉사센터</P></TD></TR></TBODY></TABLE></P>
691 <P>라는 제목을 보고 올리는건데.....</P>
692 <P>자원봉사센터가..안동인가요...??</P>
693 <P>&nbsp;&nbsp;&nbsp;</P>
694
```

● 소스코드에 주민등록번호 사용



## 2. 개인정보 유·노출 사례 및 조치

### 🔒 디렉터리 리스팅 보안설정 미흡 - 디렉터리 리스팅 취약점으로 인해 노출

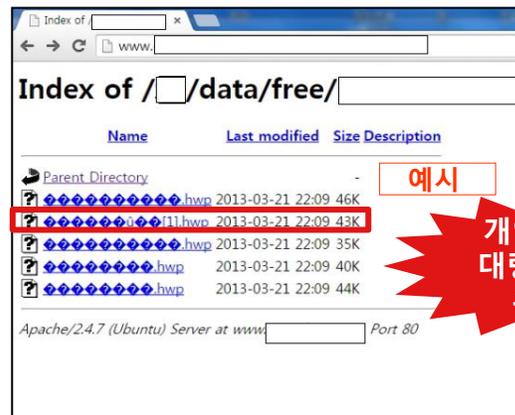
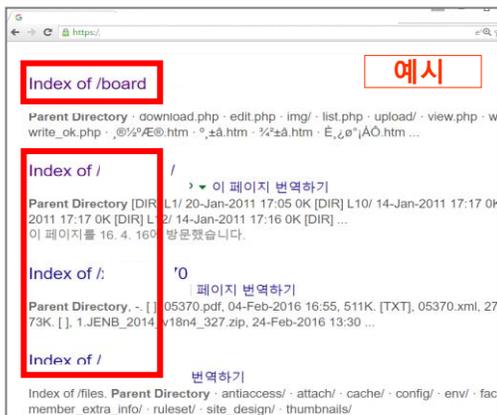
#### ▶ 디렉터리 리스팅 취약점으로 인해 노출

- 서버관리자가 사이트 테스트 목적으로 사용하는 설정으로 인터넷 사용자에게 웹 서버 내 디렉터리와 파일 목록을 보여주는 기능
- 웹 서버의 URL로 "도메인 네임 + 디렉터리" 경로를 입력 했을 때, 웹 브라우저에 해당 디렉터리 내, 모든 파일 목록이 노출되는 보안 취약점

#### ✓ 조치

- **Step 1.** 운영체제 등 서비스 환경에 맞도록 디렉터리 리스팅 취약점 조치 필요
- **Step 2.** 접근제어 설정
- **Step 3.** 디렉터리 설정 및 변경

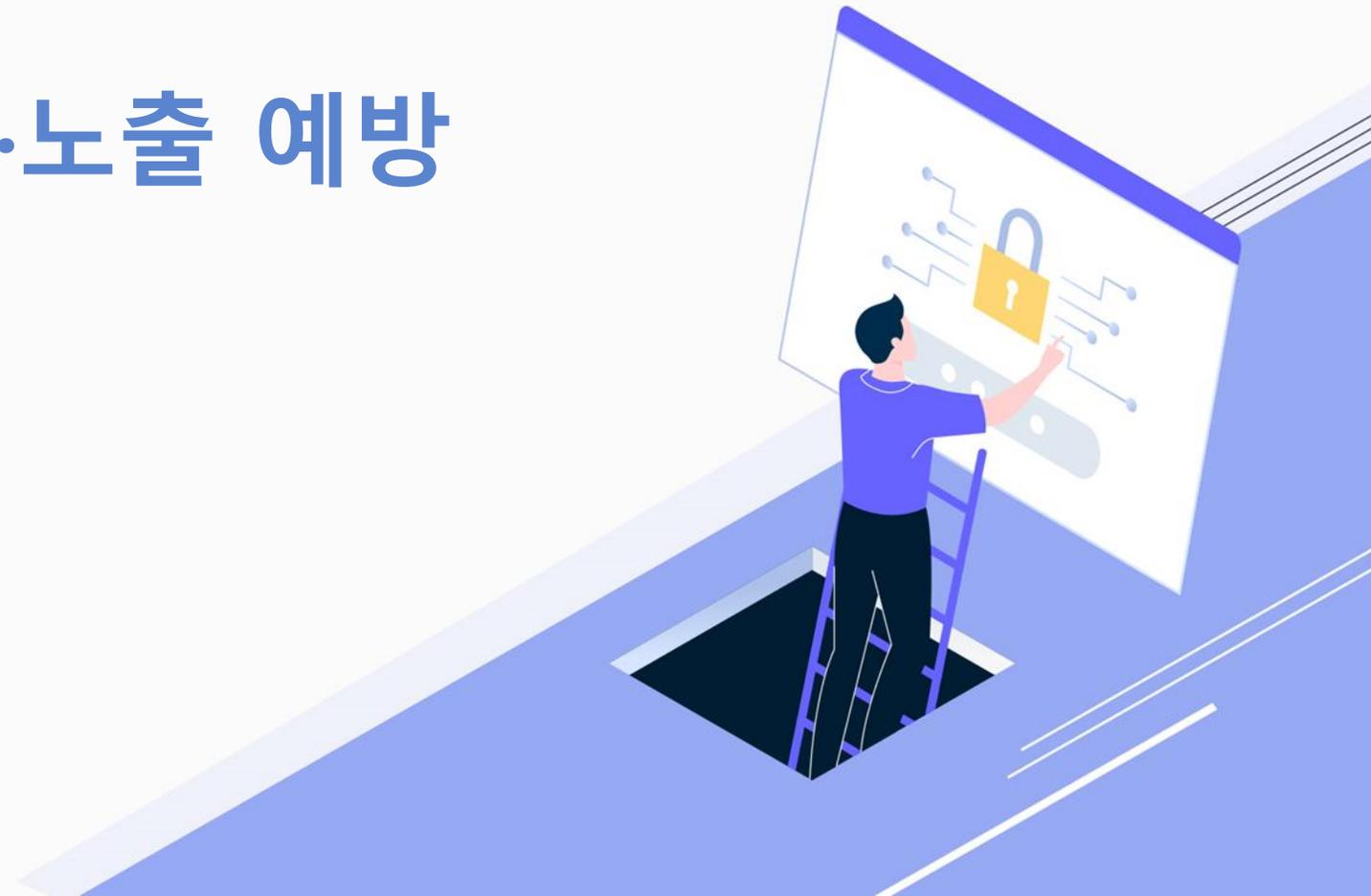
### 디렉터리 리스팅 취약점이 있는 홈페이지 검색(예시)



개인정보  
대량 노출  
위험

3

## 개인정보 유·노출 예방





## 3. 개인정보 유·노출 예방

### 🔒 안전성 확보 조치

#### ▶ 안전성 확보에 필요한 기술적·관리적 및 물리적 조치



1. 내부관리 계획의 수립 시행



2. 접근권한의 관리



3. 접근통제



4. 개인정보의 암호화



5. 접속기록의 보관 및 점검



6. 악성 프로그램 등 방지



7. 관리용 단말기의 안전조치



8. 물리적 안전조치



9. 재해·재난 대비 안전조치



10. 개인정보의 파기



## 3. 개인정보 유·노출 예방

### 🔒 개인정보 노출 예방 수칙

#### 운영자

- 게시판 운영 시 개인정보 노출 주의 **안내**
- 개인정보가 포함된 게시글 및 댓글 작성 시 **비공개** 설정
- 불가피하게 개인정보가 포함된 게시물 생성 및 게시글·댓글 작성시 **마스킹 등 비식별** 처리
- **첨부파일**을 등록하기 전 개인정보 유무 확인
- 주기적인 개인정보 **노출 점검**



#### 개발자

- 관리자페이지 **접근제어** 설정
- 게시판을 **비공개** 또는 비밀글 설정이 가능하도록 구축
- **접속경로(URL)** 설정, **소스코드** 등에 개인정보 사용 금지
- **접속경로(URL)** 식별자는 **'숨김'** 처리하여 보호
- 홈페이지 개발 및 개편 시 웹·소스코드 **취약점 점검**
- **디렉토리 리스팅** 여부를 점검





## 3. 개인정보 유·노출 예방

### 🔒 운영자 개인정보 노출 예방수칙 5계명

#### 1 게시판 운영 시 개인정보 노출 주의 안내하세요

- 서버관리자가 사이트 테스트 목적으로 사용하는 설정으로 인터넷 사용자에게 웹 서버 내 디렉터리와 파일 목록을 보여주는 기능
- 웹 서버의 URL로 "도메인 네임 + 디렉터리" 경로를 입력 했을 때, 웹 브라우저에 해당 디렉터리 내, 모든 파일 목록이 노출되는 보안 취약점

[예시]

· 운영에 부적합하다고 판단되는 글은 일일로 삭제처리되며, 게시물 내용에 따라 이동처리 할 수 있음을 알려 드립니다.

· 내용 입력시 주민등록번호, 연락처 등 개인정보가 노출되지 않도록 주의하시기 바랍니다.

제목	<input type="text"/>
작성자	<input type="text"/> <input checked="" type="radio"/> 전체공개 <input type="radio"/> 비공개
전화번호	<input type="text"/>
이메일	<input type="text"/> @ <input type="text"/> 직접 입력 <input type="button" value="v"/>
내용	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>

웹 페이지 메시지

?

게시글 작성 시 주민등록번호, 연락처 등 개인정보가 포함되지 않았는지 확인하셨습니다가?



## 3. 개인정보 유·노출 예방

### 🔒 운영자 개인정보 노출 예방수칙 5계명

#### 2 개인정보가 포함된 게시글 및 댓글 작성 시 비공개 설정하세요

- 게시글에 대한 비공개 여부를 설정할 수 있는 기능 필요
- 개인정보가 포함되는 민원 페이지나 각종 신청 관련 게시판은 비공개 설정

[예시]

접수번호	제목	작성자	등록일
37436	🔒 비공개 글입니다.	***	2018-08-01 13:55

\* 표시된 항목은 필수입력 항목입니다.

\* 제목

작성자 김\*\*\*

공개여부 비공개 공개

\* 내용

첨부파일

※파일1개당 최대10MB까지만 가능합니다

위 글 등록을 위해 기입하신 개인정보수집 및 이용에 동의합니다.(필수)



## 3. 개인정보 유·노출 예방

### 🔒 운영자 개인정보 노출 예방수칙 5계명

#### 3 불가피하게 개인정보가 포함된 게시글·댓글 작성시에는 마스킹 등 비식별 처리하세요

- 이벤트 당첨, 합격자 공개 시 개인정보 마스킹

[예시]

#### 당첨자 발표

##### 1등: 호텔 이용권 1명

박\* (010\*\*\*\*25)

##### 2등: 외식상품권 20명

박* (010****51)	구* (010****15)
우* (010****84)	백* (010****95)
구* (010****32)	이* (010****02)
손* (010****01)	설* (010****69)
구* (010****67)	이* (010****58)
이* (010****19)	김* (010****67)
배* (010****33)	배* (010****01)
정* (010****13)	이* (010****13)
류* (010****40)	김* (010****78)
신* (010****73)	신* (010****45)



## 3. 개인정보 유·노출 예방

### 🔒 운영자 개인정보 노출 예방수칙 5계명

#### 4 첨부파일을 등록하기 전에 개인정보 유무 확인하세요

- 첨부할 파일에서 불필요한 정보는 삭제 후 게시(업로드)
- 작성된 첨부 문서에서 개인정보의 포함여부 확인 후 게시(업로드)

#### 엑셀문서

- 숨겨진 Sheet/행/열에 개인정보 포함 여부 확인
- 외부 공개용 문서의 경우 함수 사용은 지양하고, 데이터의 값만 활용
- 메모에 개인정보가 있는지 확인
- OLE 객체(그래프 등)는 더블클릭 후 원본자료에 개인정보가 있는지 확인

#### 한글문서

- 한글의 "개인정보 보호 기능"(보기메뉴)을 이용하여 개인정보 유무 확인

#### 이미지파일

- 이미지 파일에 개인정보 포함 유무 확인





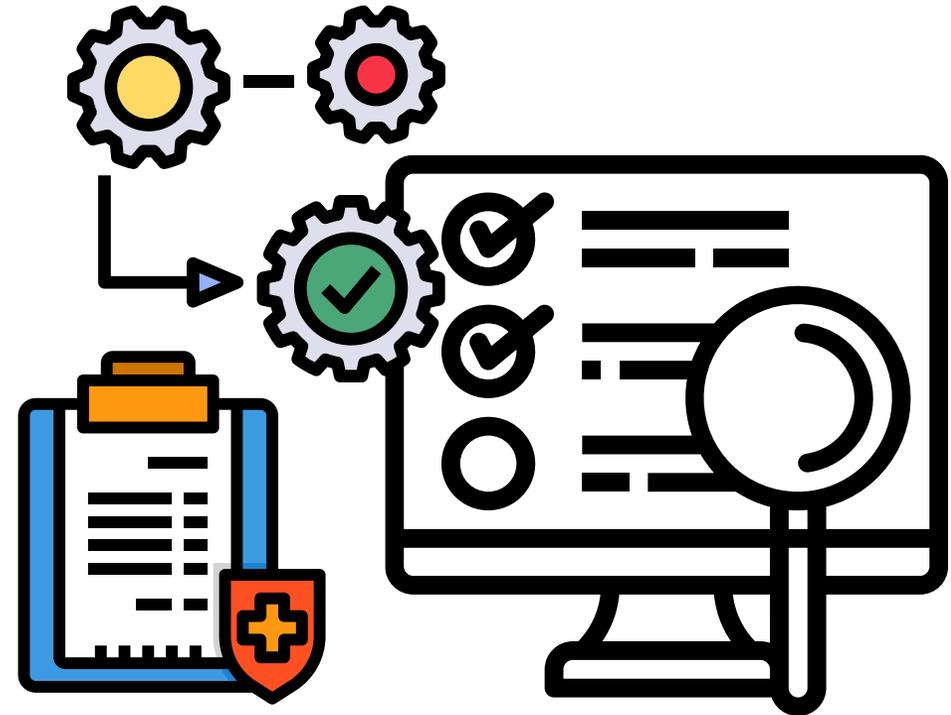
## 3. 개인정보 유·노출 예방

### 🔒 운영자 개인정보 노출 예방수칙 5계명

#### 5 주기적으로 개인정보 노출 여부를 점검하세요

- 주기적으로 아래 사항을 점검

- ✓ 검색엔진(구글, 네이버, 다음 등) 확장기능을 이용한 개인정보 주기적 점검  
(검색단어 : "번호", "주민", "전화", "여권" 등 활용)
- ✓ 개인을 구분하는 값으로 개인정보 사용여부 점검
- ✓ 전송 및 저장시 개인정보 암호화 여부 점검
- ✓ (개발 시) 시큐어 코딩을 적용하여 개발
- ✓ (개발 후) 시큐어 코딩 준수여부 점검
- ✓ 웹 취약점 점검





### 🔒 개발자 개인정보 노출 예방수칙 6계명

#### 1 관리자페이지를 안전하게 보호하세요

- 관리자페이지는 가급적 내부망에서만 연결되도록 구성
- "VPN"이나 "전용망" 등 안전한 접속수단 및 "OTP", "휴대폰", "공인인증서" 등 안전한 인증수단 적용
- 관리자페이지는 접속이 필요한 관리자만 접근할 수 있도록 인가된 IP로 제한하는 기능 적용

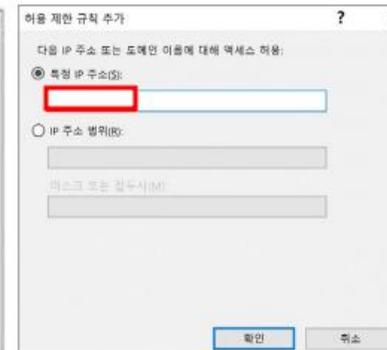
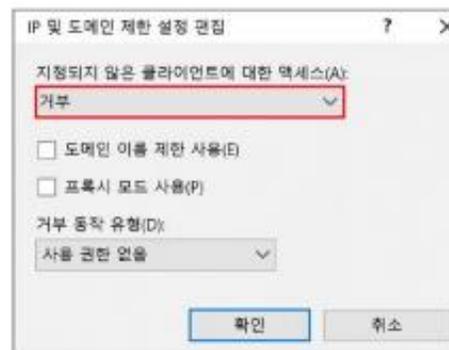
#### [예시]

##### ✓ IIS 웹 서버(윈도우즈 서버)의 경우(IIS 7.x 이상 기준)

- "설정 > 제어판 > 관리도구 > 인터넷 서비스 관리자" 선택
- 해당 관리자페이지 폴더 > IP 주소 및 도메인 이름 제한 > 기능 설정 편집
- 지정되지 않은 클라이언트에 대한 액세스를 거부로 설정(전체 접속 차단)
- 접속 허용할 IP주소 입력

##### ✓ Tomcat 서버의 경우

- \$CATALINA\_HOME(톰캣 홈 디렉터리)/conf/server.xml 파일 내용 중 <Host> 부분
- 필드 사이에 아래와 같은 설정을 추가한 후 서버를 재시작하면 관리자페이지에 대해 IP기반으로 허용된 IP만 접근이 가능하도록 제어가 가능



관리자페이지 접근제한 설정

```
<Host ...>
<Context path="/KISAadm" docBase="/tomcat/webapps/ROOT/KISAadm">
<Valve className="org.apache.catalina.valves.RemoteHostValve"
    allow="허용할 IP"/>
</Context>
</Host>
```



## 3. 개인정보 유·노출 예방

### 🔒 개발자 개인정보 노출 예방수칙 6계명

#### 2 게시판은 비공개 또는 비밀번호 설정이 가능하도록 구축하세요

- 게시글에 개인정보 포함시 비공개 또는 비밀번호로 설정할 수 있는 기능 적용
- 비밀번호는 작성자만 열람할 수 있도록 적용

[예시]

The screenshot shows a web editor interface. At the top, there are fields for '제목' (Title) and '작성자' (Author). Below these is a rich text editor with a toolbar containing various text formatting options. At the bottom of the editor, there are tabs for '편집' (Edit), 'HTML', and '미리보기' (Preview). Below the tabs, there is a '태그' (Tag) field. At the bottom, there is a '공개여부' (Public/Private) section with two radio buttons: '공개' (Public) and '비공개' (Private). The '공개' radio button is selected and highlighted with a red box. Below this section are two buttons: '입력완료' (Input Complete) and '취소' (Cancel).



### 개발자 개인정보 노출 예방수칙 6계명

#### 3. 접속경로(URL) 설정, 소스코드 개발 등에 개인정보를 사용하지 마세요

- 회원정보 페이지 개발 시 접속경로(URL)에 생년월일, 주민등록번호 등 사용 금지  
ex) <http://www.test.or.kr/board.php?search=info&list=19810101>
- 소스코드 내에 회원 식별자로 주민등록번호 등 사용 금지

[예시]

```
<td width="50%" height="10">작성자 : 주███</td><a href='?cmd=reply&info_idx=1&member_pno=880924'>sb
```



```
<td width="50%" height="10">작성자 : 주███</td><a href='?cmd=reply&info_idx=1&member_no=1004_com=yes&gu
```

#### 4. 접속경로(URL) 식별자는 '숨김' 처리하여 보호하세요

- URL내 개인정보 등이 노출되지 않도록 POST 방식을 이용  
ex) <http://www.test.or.kr/board.php?search=info&list=19810101>

- ✓ 홈페이지 설계 시 페이지 구분 값 등으로 개인정보를 사용하는 경우 URL에 개인정보가 노출됩니다.  
웹브라우저 주소 표시줄에 개인정보가 노출되지 않도록 GET 방식 보다는 POST 방식을 사용해야합니다.



## 3. 개인정보 유·노출 예방

### 개발자 개인정보 노출 예방수칙 6계명

#### 5 홈페이지 개편 시 웹·소스코드 취약점 점검하세요

- 소스코드 내 개인정보 포함여부 점검
- 소스코드 주석, 개발/테스트를 위한 에러 메시지 등에 서버정보 포함여부 확인

[예시]

#### Forbidden

You don't have permission to access / on this server.

Apache/2.2.3 (CentOS) Server at ~~10.10.10.10~~ Port 80

에러 페이지 내 서버정보 포함

```
29 /*본인요청으로 삭제(2017.11.09)*/  
30 /*if('=="topstand" && ' == "2") {alert("실명제 적용에 따라 '반정민'님은 '오정민'님으로  
31 성명이 변경처리 되었습니다.\n\n이와 관련하여 문의사항은 전산과 10.10.10.10로 연락주시기 바랍니다.");}*/
```

웹페이지 소스코드 주석

- ✓ 모든 웹 페이지에 대해 개발단계에서 디버깅 및 테스트를 목적으로 작성한 주석구문에 서버 주요 정보가 포함되어 있을 경우 공격자가 해당 정보를 다른 취약점과 연계해 사용할 수 있으므로 제거해야 합니다.



## 3. 개인정보 유·노출 예방

### 🔒 개발자 개인정보 노출 예방수칙 6계명

#### 6 디렉토리 리스팅 여부를 점검하세요

- 주기적인 점검 기본사항
- 디렉터리 리스팅 노출 방지 설정

- ✓ 검색엔진(구글, 네이버, 다음 등) 확장기능을 이용하여 내 홈페이지의 관리자페이지가 리스팅 되고 있는지 주기적 점검  
(웹 서버의 url로 "도메인네임 + 디렉터리" 경로를 입력하여 웹브라우저에 해당 디렉토리 등 모든 파일목록이 노출되는지 점검)
- ✓ Apache
  - indexes "문자열"제거
- ✓ Tomcat
  - Param-value 값을 "False" 로 설정
- ✓ Nginx
  - Autoindex 값을 "off"로 설정
- ✓ 윈도우 인터넷 정보서비스(IIS)
  - 제어판 > 관리도구 > 인터넷서비스 관리자 > 기본 웹사이트 속성 정보 수정(디렉터리 검색 부분을 비활성화)

감사합니다

