개인정보 유 · 노출 사고 사례 및 대응방안

KISA 한국인터넷진흥원

KISA 한국인터넷진흥원

목차

CONTENTS

Ⅰ. 개인정보 유·노출 개념 및 현황

Ⅱ. 개인정보 노출사례 및 조치방안

Ⅲ. 개인정보 노출 점검 실습

Ⅳ. 개인정보 유출 사례 및 조치방안

Ⅴ. 개인정보 유출사고 조치 및 책임

Ⅰ. 개인정보 유·노출 개념 및 현황

1. 개인정보 “노출” 및 “유출” 정의
2. 개인정보 유 · 노출 시 조치사항
3. 개인정보 유 · 노출 현황 및 사고원인
4. 개인정보 유 · 노출 피해
5. 개인정보 유출 사고 사례
6. 개인정보 노출 사고 사례

1. 개인정보 “노출” 및 “유출” 정의

“개인정보” 『노출』 이란?

홈페이지 상 개인정보를 누구든지 알아볼 수 있어
개인정보 유출로 이어질 수 있는 상태로
아래와 같은 경우

① 개인정보가 포함된 게시물이
누구든지 알아볼 수 있는 상태로 등록된 경우

② 이용자 문의 댓글에 개인정보가
공개되어 노출이 된 경우

③ 개인정보가 포함된 첨부파일을
홈페이지 상에 게시한 경우

“개인정보” 『유출』 이란?

정보주체의 “개인정보”에 대하여 개인정보처리자가
통제를 상실하거나 또는 권한 없는 자의 접근을
허용한 경우로서 다음 어느 하나에 해당하는 경우

※ 표준 개인정보 보호지침 제25조

① 개인정보가 저장된 DB 등 개인정보처리시스템에
정상적인 권한이 없는 자가 접근한 경우

② 개인정보처리자의 고의 또는 과실로 인해
개인정보가 포함된 파일, 문서, 저장매체 등이
잘못 전달된 경우

③ 개인정보가 포함된 서면, 이동식 저장장치,
휴대용 컴퓨터 등을 분실하거나
도난을 당한 경우

2. 개인정보 유·노출 시 조치사항

1. 신속히 노출 페이지 삭제 또는 비공개 처리
2. 검색엔진에 노출된 개인정보 삭제 요청 및 로봇 배제 규칙 적용(외부검색엔진의접근차단)
3. 시스템의 계정, 로그 등을 점검 후 분석결과에 따른 접속 경로 차단(제3자접근여부파악)
4. 재발방지를 위해 서버, PC등 정보처리시스템의 백신을 최신으로 업데이트 후 디렉토리 점검

1. 유출된 정보주체에게 지체 없이 통지(5일이내)
   ※ 정보통신서비스 제공자등의 경우 "24시간 이내"
   - 유출된 개인정보의 항목 (필수항목)
   - 유출된 시점과 그 경위
   - 피해 최소화를 위한 정보주체의 조치방법
   - 기관의 대응조치 및 피해구제 절차
   - 피해 신고 접수 부서 및 연락처
2. 피해 최소화를 위한 대책 마련 및 필요한 조치 실시
3. 1천명 이상의 개인정보가 유출된 경우
   ※ 정보통신서비스 제공자등의 경우 "1건 이상"
   국가(개인정보보호위원회 또는 한국인터넷진흥원)에 신고하고 개인정보 유출 사실을 홈페이지에 7일 이상 게재
   ※ 유출신고: 개인정보보호 종합포털(www.privacy.go.kr) 등

3. 개인정보 유·노출 현황 및 사고원인

유출, 침해의 초 대량화

개인정보 대량집적 추세
→ 유출사고 초 대량화 (천만~억 건)

전국민의 개인정보 유출 위험

개인정보 취급분야 확대

(기존)정보통신업 + { 기타 사업분야 / 비영리단체 등

다양한 분야에서 문제 발생 가능

새로운 기술 발달

스마트폰, 클라우드 컴퓨팅,
CCTV, AI, 빅데이터 등

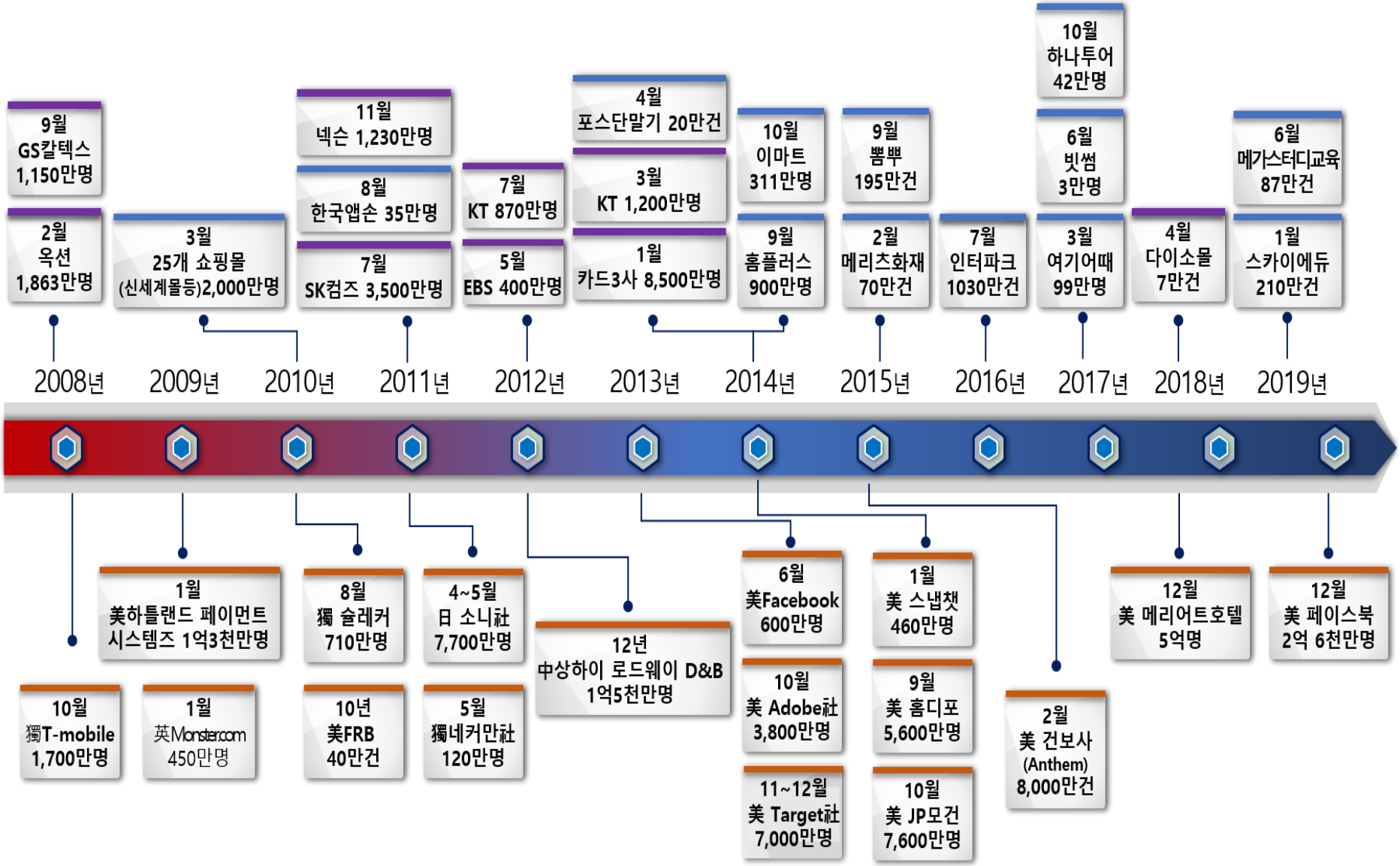
**새로운 기술에 기반한
심각한 이슈 발생**

정보 주체의 인식 변화

집단소송, 분쟁조정, 침해신고 등
개인정보 침해에 적극적 대응

정보주체의 권리보장 요구 증대

3. 개인정보 유·노출 현황 및 사고원인



4. 개인정보 유 · 노출 피해

개인정보 침해에 따른 개인/기업/국가의 피해

개인

정신적 피해뿐만 아니라 명의도용, 보이스피싱에 의한 금전적 손해, 유괴 등 각종 범죄에 노출

기업

기업의 이미지 실추, 소비자단체 등의 불매운동, 다수 피해자에 대한 집단적손해배상시 기업 경영에 큰타격

국가

프라이버시 라운드의 대두에 따른 IT산업의 수출애로, 전자정부의 신뢰성 하락, 국가브랜드 하락

4. 개인정보 유 · 노출 피해

개인정보 수집 · 이용

- 통신사 포털
- 호텔 백화점
- 은행 카드사
- 의료기관, 동호회
- 웹사이트

개인정보 유출

- 내부자 · 위탁직원

USB등으로 무단 유출

- 해커

→ SQL인젝션

→ 웹쉘 업로드

→ URL인덱스 취약점

→ APT 공격

- 관리부주의

→ 홈페이지 보안조치 미흡

→ 메일 오발송

개인정보 축적 · 거래

- 온라인

→ 인터넷 카페 등을 통한 거래

- 오프라인

→ CD등 저장매체를 통한 직접 판매

개인정보 오남용

- 명의도용
- 불법 대포 폰 개설
- SMS 등 불법 스팸
- 과도한 TM

4. 개인정보 유 · 노출 피해

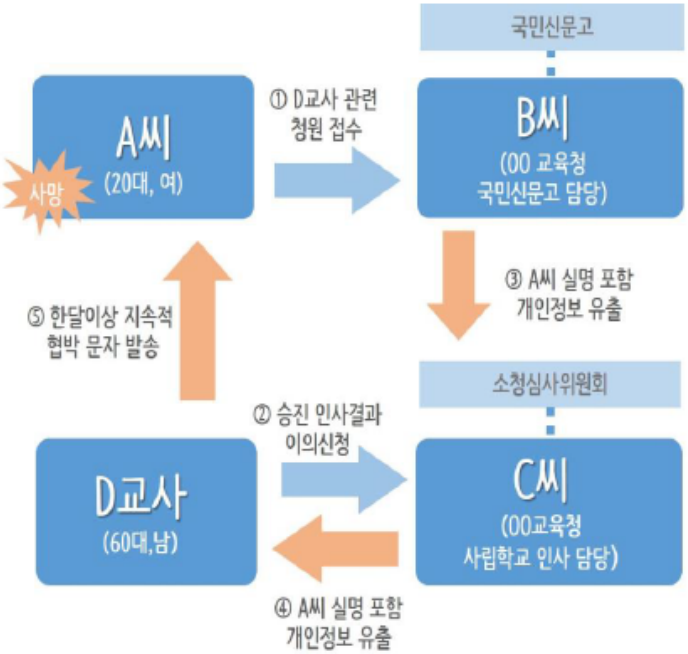
사 례

(개인) 개인정보 유출로 인한 정신적 피해

'개인정보 유출' 공익제보자 결국…경찰, 담당 공무원 입건

공익제보자가 자신의 개인정보가 유출된 것을 알고 끝내 스스로 목숨을 끊은 A씨의 사건과 관련해 경찰이 담당 공무원들을 입건했다. OO경찰서는 국민신문고 청원자 개인정보를 삭제하지 않고 외부로 유출한 혐의(개인정보 보호법 위반)로 OO교육청 직원 B씨와 도교육청 산하 교원소청심사위원회 직원 C씨를 입건했다고 27일 밝혔다. 경찰은 청원자에게 협박성 문자메시지를 보낸 혐의(협박)로 전직 교사 D씨도 입건했다.

(출처: 연합뉴스TV, 2018.12.26.)



4. 개인정보 유 · 노출 피해

사 례

(개인) 생명 위해(危害) 우려

OO센터 PC 해킹…탈북민 997명 개인정보 유출

탈북민의 성명·생년월일·주소 담김 파일 유출!

이번 해킹을 주도한 해커의 신원과 목표가 아직 밝혀진 게 없는 상황이라 탈북민들은 불안감을 감추지 못했다

탈북민들 개인정보 유출에 잠 못 드는 이유… "개인정보 유출? 북한에 있는 가족들 신변이 더 위험하다."

(출처: 한겨레, 2018.12.28.)

(사진: 연합뉴스)

4. 개인정보 유 · 노출 피해

사 례

(개인) 개인정보 도용 피해

2015년 도박 혐의로 검거 된 A씨는 1984년 절취한 B씨의 신분증과 학생증으로 B씨의 신분을 도용하여 살아왔으며, 1987년 항정신성의약품위반죄로 징역 1년, 2015년 즉결심판 청구 되었음, 이에 B씨는 신분도용의 피해를 우려하여 주민등록번호 변경결정 청구, 이에 주민등록번호변경 심의위원회는 변경결정 신청을 받아 들임

(출처: 행정안전부, 주민등록번호 변경결정 사례집, 2018.12.18.)

4. 개인정보 유 · 노출 피해

사 례

(기업) 개인정보 유출로 인한 손해배상 및 이미지 실추

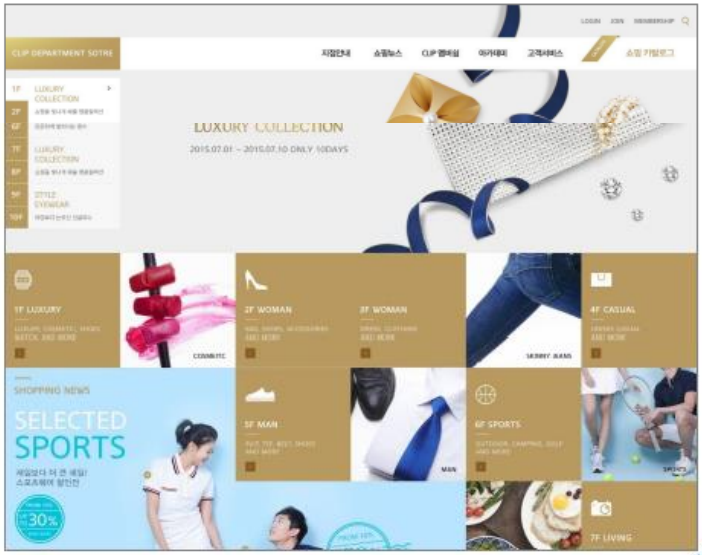
'개인정보 유출' OO 인터넷 쇼핑몰 , 45억 과징금

2016년 개인정보 유출 사건으로

45억원 상당 과징금을 부과 받은 OO 인터넷

쇼핑몰이 처분이 부당하다며 소송을 제기했지만

받아들여지지 않았다.



(출처: 중앙일보, 2018.7.5.)

5. 개인정보 유출 사고 사례

다중 이용 서비스·솔루션 취약점에 의한 개인정보 유출

유출사례(1)

- **고객사 개인정보 유출**로 연결
- 개인정보보호 관련 법령에는 고객사가 위탁사이며, **관리·감독 책임**이 있음

보안뉴스 미디어

[redacted] 제작 웹 솔루션, SQL 인젝션 취약점 발견

2018-03-11

[redacted]에서 제작한 쇼핑몰 웹 솔루션에서 SQL Injection 취약점 발견
PC&Mobile 쇼핑몰 파라미터 유효성 검증 게시 글 확인해 업데이트 적용해야

[보안뉴스 김경애 기자] [redacted]에서 제작한 쇼핑몰 웹 솔루션에서 SQL Injection 취약점이 발견됐다. 이에 따라 eLnPU 독립형 시즌 4 이하 제품 이용자는 보안 업데이트가 필요하다.

▲취약점 패치 안내 화면(이미지 [redacted]

보안뉴스 미디어

[redacted]소프트, DB 해킹 당해 개인정보 유출됐다

2019-11-24

[redacted]소프트, 지난 10일경 해커에 의해 DB 공격 당해 개인정보 유출 정황 확인
이름, 아이디, 비밀번호, 이메일, 연락처, 주소 등 총 6개 항목 유출

[보안뉴스 김경애 기자] 온라인 쇼핑몰에 웹 호스팅 및 DB 호스팅 서비스를 제공하는 [redacted]소프트가 해킹을 당해 개인정보가 유출되는 사건이 발생했다.

(이미지=clickart)

[redacted]소프트에 따르면 지난 11월 10일경(추정) 심야불상의 해커가 DB를 해킹해 개인정보를 빼낸 정황을 확인했다. 현재 서울지방경찰청과 관계기관에서 수사가 진행중이라며, 정확한 해킹 일시 등 관련사항이 확인되면 추가로 알리겠다고 밝혔다.

5. 개인정보 유출 사고 사례

가상통화거래소 등 新 서비스 해킹에 취약

유출사례(2)

- 가상통화거래소, O2O 등 **인터넷 기반 新 서비스가 해킹에 여전히 취약**
- 가상통화 거래소 10개사 현장조사 후 **8개사 처분**(2개사는 서비스 중단)

보안뉴스 미디어

3년간 해킹으로 암호화폐 1,121억원 부정 인출

2018-10-04

2016년 1건 3억원, 2017년 4건 405억원, 2018년 2건 713억원
암호화폐 개인지갑 해킹 158건...올해만 91건, 검거는 6건 불과

[보안뉴스 김경애 기자] 국내 암호화폐 거래소의 해킹사고가 끊임없이 발생하고 있는 가운데, 범인 검거율과 함께 암호화폐 거래소의 보안은 여전히 미흡한 것으로 드러났다.

행정안전위원회 대한애국당 조원진 의원이 3일 경찰청으로부터 제출받은 최근 3년간 가상통화 거래소 해킹 피해 현황 및 조치 내역에 따르면, 2016년 이후 7번의 해킹 사건이 발생했다. 해킹을 통해 부정인출된 금액만 무려 1,121억원에 달하는 것으로 밝혀졌다.

방송통신위원회

보 도 자 료

2018년 1월 24일(수) 14시부터 보도하여 주시기 바랍니다.

제공일: 2018.1.24.(수)

하나 된 열정 하나 된 대한민국

문의 : 이용자정책국 개인정보침해조사과 천지현 과 장(☎2110-1567)
선주열 사무관(☎2110-1518)

방통위, [redacted] 등 가상통화 거래사이트 운영 8개사에 과태료 및 시정명령 처분

- 가상통화 거래사이트, 개인정보 보호조치 매우 미흡 -

방송통신위원회(위원장 이효성)는 1월 24일(수) 제5차 전체회의를 개최하여 가상통화 거래사이트를 운영하는 사업자 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 을 위반한 것으로 나타난 **8개 사업자**에 대해 **△과태료 총 1억4천1백만원, △위반행위 즉시중지 및 재발방지 대책 수립 보고** 등 시정명령을 하기로 의결하였다.

5. 개인정보 유출 사고 사례

단순 해킹 공격, 관리자 실수에 의한 유출 사고

유출사례(3)

- 정부가 국내 300만 개인정보처리자/정보통신서비스사업자 전체 관리는 불가
- 개인정보보호에 대한 지속적인 투자 및 관심 미흡으로 **단순해킹(홈페이지 취약점), 관리자 실수(이메일 동보 발송 등)**에 의한 개인정보 유출이 지속 발생

❖ 홈페이지 게시판의 파일 업로드 취약점을 이용하여 웹셸 업로드 후 개인정보처리시스템(DB)에 접근, 회원 정보를 탈취

- 쇼핑몰(08), 금융사(11), 방송국(12), 소셜커머스(14), 커뮤니티(15)

❖ 홈페이지 취약점(URL파라미터 변조, SQL-인젝션)을 이용해 타인의 개인정보를 탈취

- 통신사(12, 14), 항공사(16), 숙박앱(17)

[redacted]채용 불합격자 2000여명 개인정보 노출

직원 실수로 이메일 '개별발송' 대신 전체발송
불합격자 이름-이메일 주소 서로 공개돼

강다영 기자 | 입력 : 2018.11.29 14:53:32

[redacted]이 사원 공개채용 과정에서 불합격자 2000여명에게 실수로 불합격자 전원의 이름과 이메일 등 개인정보를 노출했다.

[redacted]진흥원, 채용형 인턴 지원자 개인정보 유출로 '곤혹'

2018-11-27

지원자들에게 다른 지원자들 개인정보 발송돼
유출된 개인정보 항목은 이름과 이메일 주소
공공기관의 개인정보보호 실태 도마 위

5. 개인정보 유출 사고 사례

내부인에 의한 고의적인 개인정보 유출

유출사례(4)

- 업무편의를 위해 권한 없는 자와 개인정보처리시스템 **계정 공유**
- 개인정보 보호의 중요성을 인지하지 못하고, 무관심 및 관리 감독 소홀로 개인정보 유출

'박사방' 공익들에 개인정보 조회 ID준 공무원들 입건

CBS노컷뉴스 윤준호 기자 | 2020-04-07 10:27 뉴스듣기 0 0 가

[redacted] 한 주민센터 [redacted]구청 공무원 입건
도운 공익들이 쓴 공무원 ID 주인
공익에게 ID 알려줬나…경찰, 곧 소환조사

사회복무요원에 개인정보 열람시킨 공무원 3년 이하 징역

개인정보 무단 조회한 사회복무요원 경고 후 고발
고발되면 복무기간 5일 연장, 법적 처벌도 강화

[헤럴드경제=김수한 기자]공무원이 사회복무요원에게 민원인의 개인정보를 열람할 수 있도록 정보시스템 접근 권한을 양도 또는 대여할 경우 3년 이하 징역 또는 3000만원 이하 벌금에 처해진다.

5. 개인정보 유출 사고 사례

- 개보법 시행(11.9.30.) 이후 '19년까지 개인정보 유출 신고는 총 150건

  * 개보법 신고 기준 변경(1만건→1천건, '17.10.19.~), 해킹 등 외부 공격 확대로 신고건수 급증

유출사고 신고 유형별 현황

구분	계	해킹	고의유출	업무과실	불법매매
2011	1	1	0	0	0
2012	12	10	1	1	0
2013	6	2	2	0	2
2014	40	31	3	3	3
2015	8	4	1	3	0
2016	0	0	0	0	0
2017	14	10	1	3	0
2018	32	15	1	16	0
2019	37	14	0	23	0
계	150	87	9	49	5

5. 개인정보 유출 사고 사례

- ICT 발전, 인터넷 확산으로 개인정보 처리가 급증하면서 '개인정보=돈'

  * 유출된 개인정보를 대가로 비트코인을 요구하거나, 개인정보DB를 불법적으로 거래

- 개인정보 유출(150건)의 58%가 해킹 등 외부 공격이 원인

개인정보 유출 사고 주요 원인

해킹[1]	업무과실[2]	고의유출[3]	불법매매[4]
58%	32.7%	6%	3.3%
87건	49건	9건	5건

1) 웹셸 업로드, 파라미터 변조, 지능형지속공격, SQL인젝션 등 해킹공격

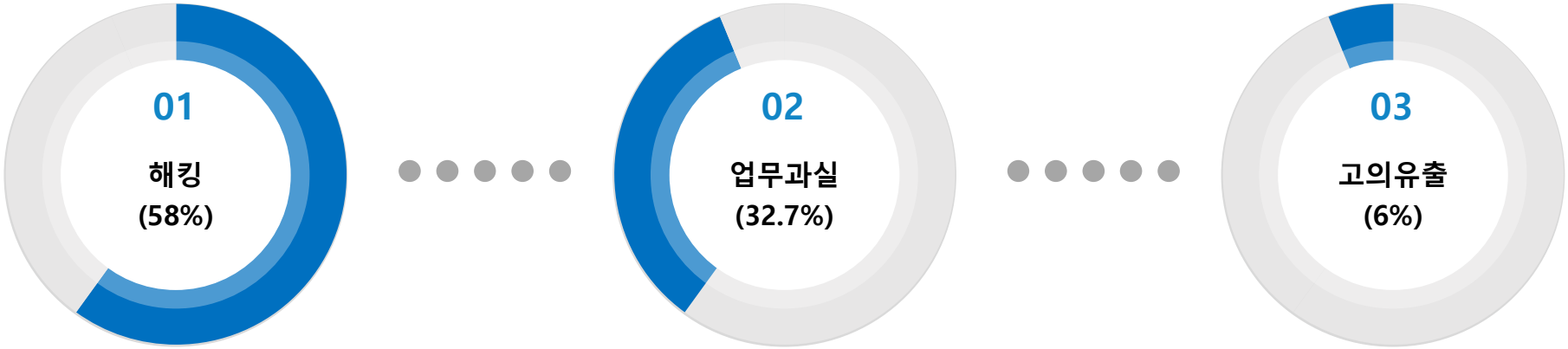
2) 이메일 오발송, 인트라넷 게시글이 구글 검색엔진에 노출, 접근통제 등 보안조치 미흡

3) 퇴사 시 USB로 다운로드 및 마케팅에 활용, 지자체 공무원이 이장에게 무단 제공 등

4) 흥신소, 다크웹 등을 통한 개인정보 매매

5. 개인정보 유출 사고 사례

개인정보 유출사고 원인 Top 3



해킹

- 웹셸 업로드, 파라미터 변조, SQL인젝션 등 해킹공격

업무과실

- 담당자 실수로 인한 이메일 오발송
- 접근통제 미흡으로 구글 검색엔진 노출

고의유출

- 퇴사 시 USB로 개인정보 다운로드
- 흥신소를 통한 개인정보 파일 구매
- 업무담당자가 지인에게 무단 제공

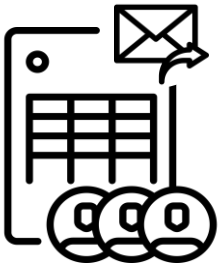
6. 개인정보 노출 사고 사례

엑셀 기능 사용 노출

1

외부파일 참조 기능을 이용해 면접 안내 파일을 작성

2



상단의 파일명을 복사한 뒤 함수창에 입력

3

지원자 전체의 개인정보가 노출

이미지 파일 노출

1

구글, 네이버, 다음 등 검색엔진에서 개인정보 키워드검색

2

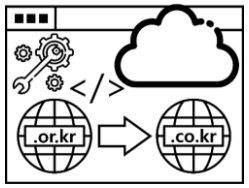
OCR 기술을 통해 개인정보가 담긴 PDF파일 검색 가능

3

홈페이지 게시판에 주민등록번호가 담긴 첨부파일 노출

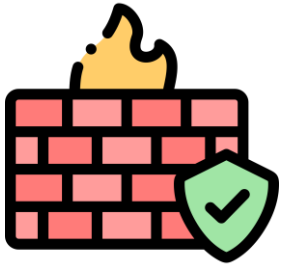
서버 이전 등 관리자 부주의 노출

1



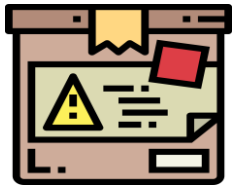
새로운 서버로 이전하며 이전 서버를 방치

2



접근통제 미설정 및 파라미터 노출로 비인가자 접근 가능

3



관리자 페이지 개인정보 노출

6. 개인정보 노출 사고 사례

1 google검색 중 구청 홈페이지 접속

2 URL 주소 한자리만 바꾸면 타인의 문서가 다운로드됨

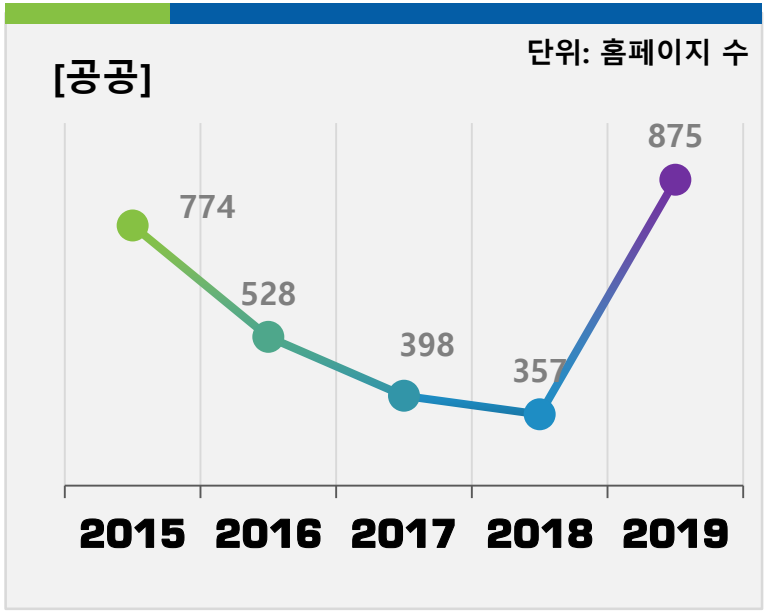
3 개인정보가 담긴 파일을(신분증, 이력서 등) 누구든지 확인가능

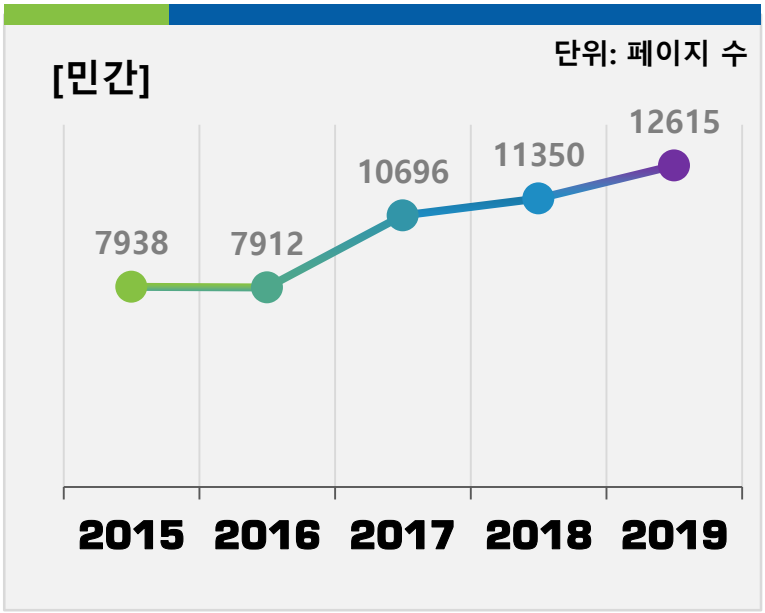
6. 개인정보 노출 사고 사례

최근 5년간 개인정보 노출 탐지 · 삭제 현황(공공, 민간)

개인정보 노출·탐지 경향

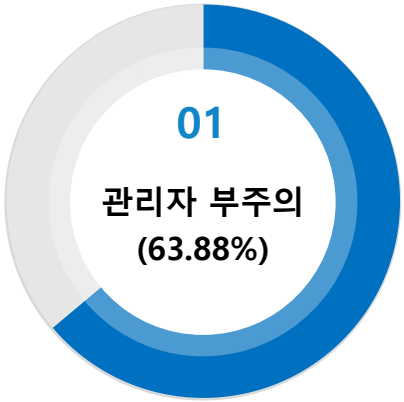
- (공공) 개인정보 노출 탐지·삭제 홈페이지는 15년도 이후 감소추세였으나, 19년도 탐지 유형 확대(4→8종)로 인해 증가
- (민간) 16년도 이후 개인정보 노출 탐지·삭제 페이지는 지속적으로 증가하는 추세로 나타남

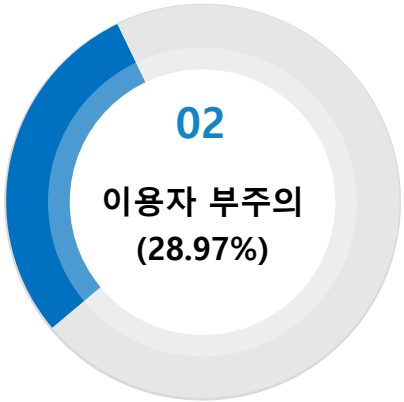


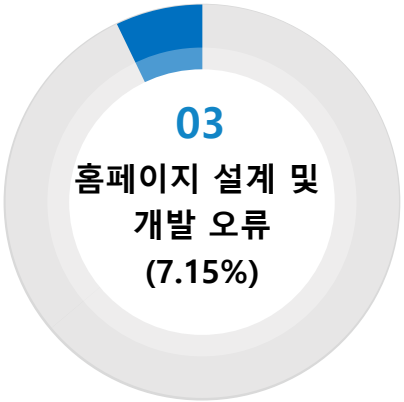


6. 개인정보 노출 사고 사례

2019년도 홈페이지 노출 원인 Top 3







홈페이지 관리자 부주의

- 개인정보 포함된 게시글 및 댓글 게시
- 개인정보가 포함된 첨부파일 게시

홈페이지 이용자 부주의

- 개인정보가 포함된 게시글 및 댓글 작성
- 개인정보가 포함된 첨부파일 게시

홈페이지설계 및 개발 오류

- 관리자페이지 접근제어 미흡
- 홈페이지 접속경로(URL) 관련 오류
- 홈페이지 소스코드 보안설정 미흡
- 디렉터리 리스팅 보안설정 미흡

Ⅱ. 개인정보 노출사례 및 조치방안

1. 홈페이지 관리자 부주의
2. 홈페이지 이용자 부주의
3. 홈페이지 설계·개발 오류

KISA 한국인터넷진흥원

개인정보 노출사례 ①

홈페이지 관리자 부주의

1. 개인정보가 포함된 게시물 게시

게시글, 댓글 및 첨부파일 인한 개인정보 노출

노출사례(1)

- 관리자의 게시글 및 댓글로 인한 개인정보 노출

○ 신기술개발자

- 회사명 : [redacted]
- 대표자 : [redacted]
- 법인(주민)등록번호 : 110111 [redacted], 750505- [redacted]
- 주 소 : 서울시 송파구 [redacted], 서울시 강남구 [redacted]

○ 신기술 내용 및 범위

- [redacted] 공동접지기술

○ 신기술 보호기간 : 지정·고시일로부터 3년

다음글	[redacted] 전원개발사업실시계획(변경)
이전글	[redacted] 품질경영 및 공산품안전관리법 시행령 전부개정령

작성자 : 김[redacted] 작성일 : 2018.06.29 방문 : 10

제목 : 외국인 등록번호로 회원가입

안녕하세요.

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

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

관리자님 글 확인하시면 전화좀 부탁드리겠습니다.

[다음글] 다음글이 없습니다.
[이전글] 이전글이 없습니다.

목록 답변 수정 삭제

한줄답변

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

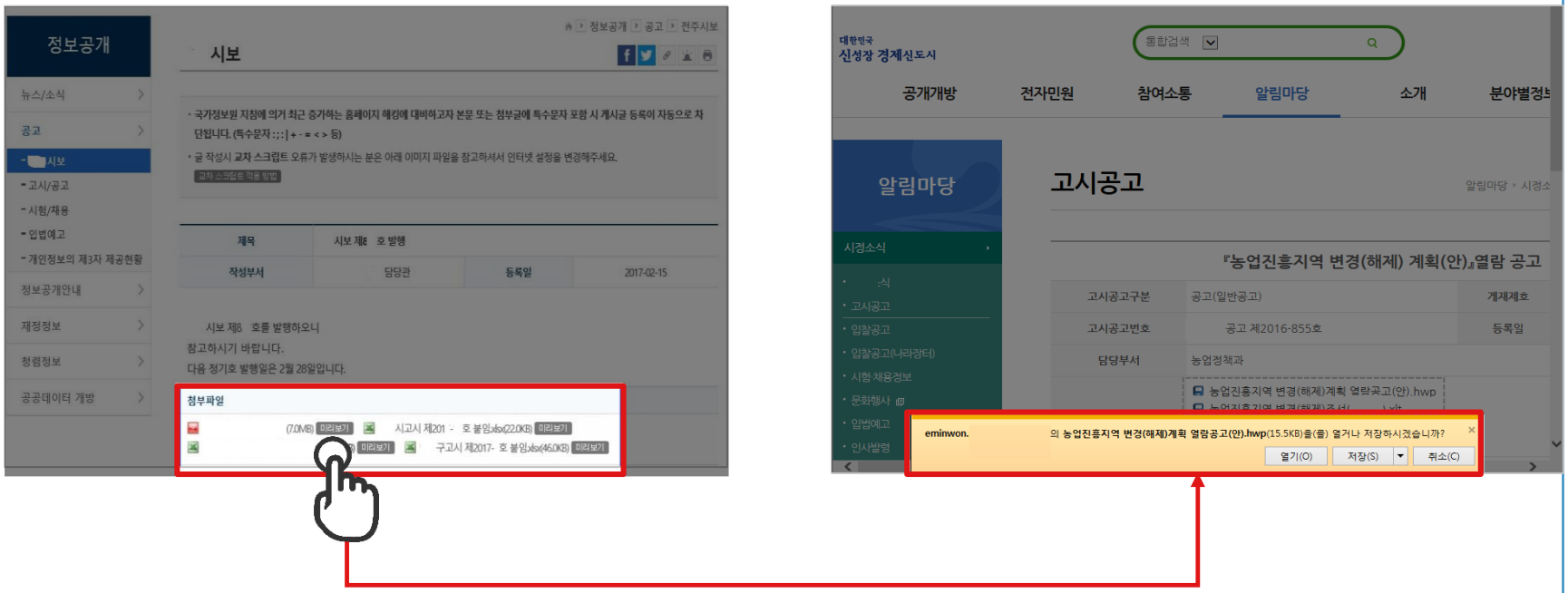
수정 삭제

1. 개인정보가 포함된 게시물 게시

게시글, 댓글 및 첨부파일 인한 개인정보 노출

노출사례(2)

- 개인정보가 포함된 파일을 첨부하여 게시판에 게시



<클릭 시, "저장" 가능>

1. 개인정보가 포함된 게시물 게시

게시글, 댓글 및 첨부파일 인한 개인정보 노출

조치방법(1)

- 비공개 게시판으로 운영

온라인상담

번호	제목	작성일
1132	주택 세금 문의	2018-10-29
1131	일반임대사업자에서 주택임대사업자로 전환할 경우에 대해서... 1	2018-10-26
1130	대형폐기물 1	2018-10-26
1129	동일한 내용의 행정소송이 최종 승소할 경우 1	2018-10-26
1128	건물 용도변경 관련 1	2018-10-26
1127	사업자신고 확인 1	2018-10-25

등록

1. 개인정보가 포함된 게시물 게시

게시글, 댓글 및 첨부파일 인한 개인정보 노출

조치방법(2)

- 최소한의 개인정보 기재 및 마스킹 처리
- 정기적인 노출 여부 확인 및 저장된 페이지 삭제

아이디 불법거래 이용자 신고제 이벤트 당첨자를 발표합니다!
페이스북 공유 이벤트 당첨자분들은 개별 메시지로,
제보를 해주신 당첨자분들은 신고해주신 메일 계정으로 안내드릴테니, 연락을 받으신 분들만 7월 10일 (수)까지 당첨 본인의 정보를 회신주시기 바랍니다. 참여해주신 분들 모두 감사합니다:)

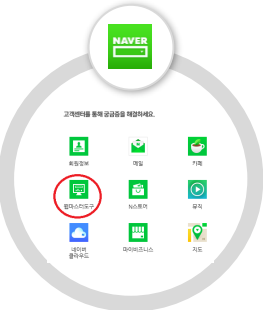
==========
o 게시글 공유자: 아이스 아메리카노(10명)
- 연*현
- 강*수
- 허*운
- 선*김
- 정*수
- 장*영
- 도*훈
- 허*이
- 이*하
- 차*호

https://www.google.com/webmasters/tools/removals

오래된 콘텐츠 삭제

https://cs.daum.net/redbell/top.html

권리침해신고

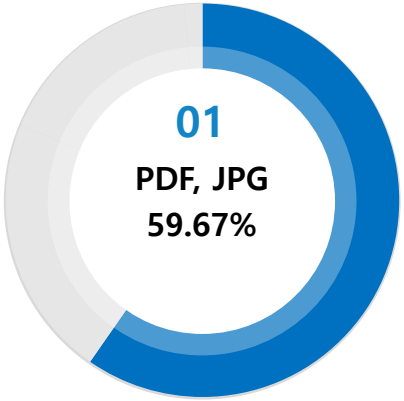


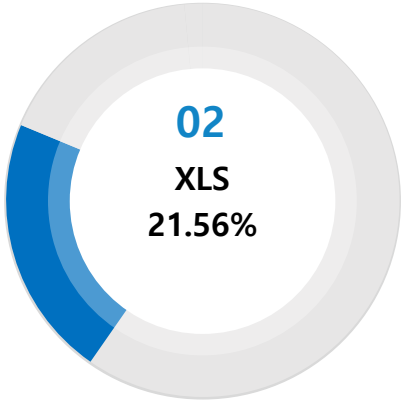
https://help.naver.com/support/home.nhn

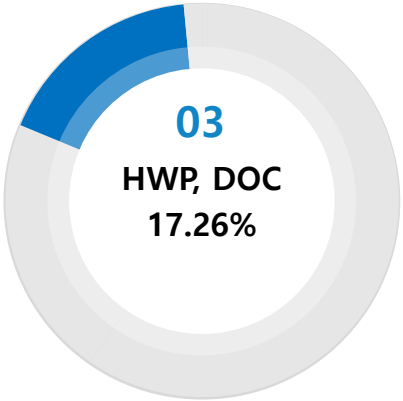
웹마스터도구

2. 개인정보가 포함된 첨부파일 게시

2019년도 홈페이지 첨부파일 노출 유형 Top 3







이미지	한글 · 워드
▪ 이미지 파일에 “개인정보” 포함	▪ 한글, 워드파일에서 노출된 “개인정보”

엑셀

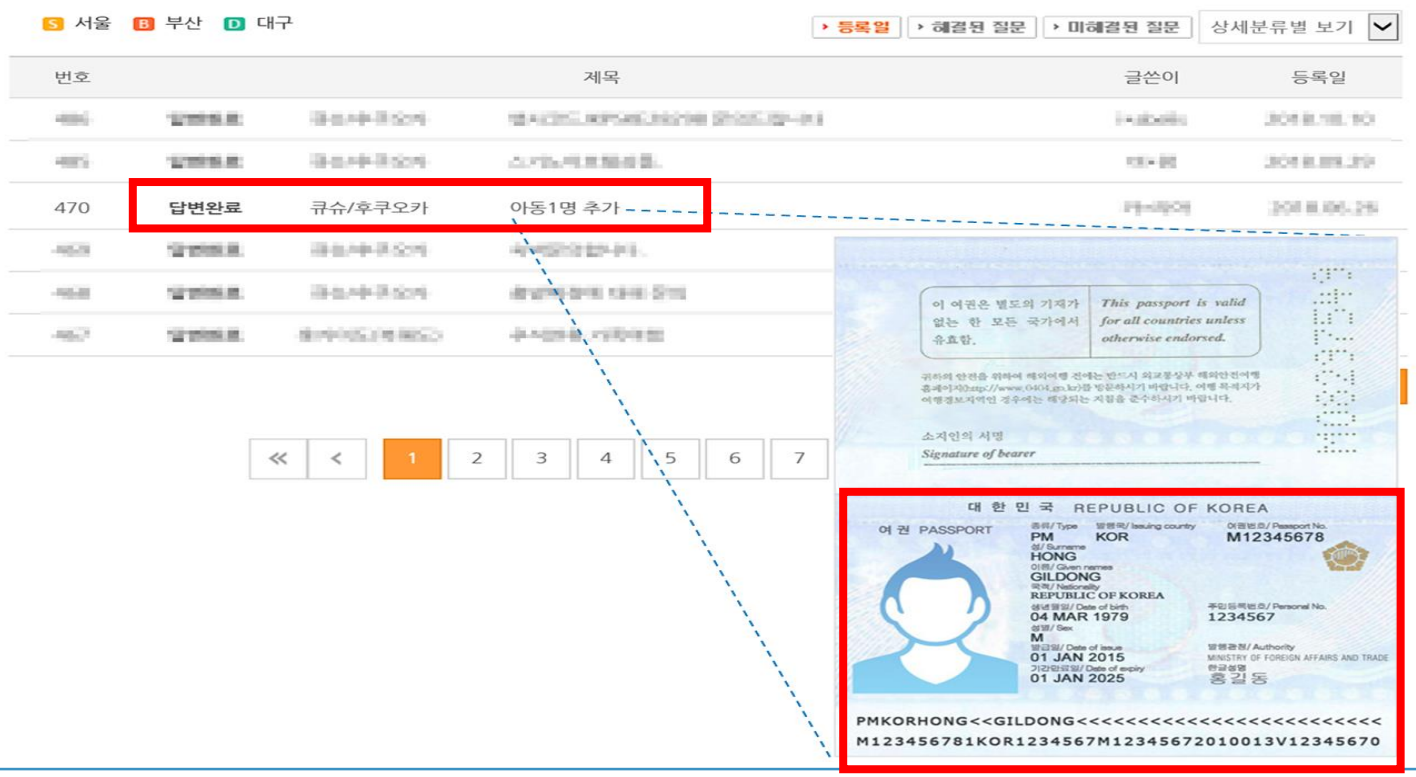
- 글자색을 배경색과 같게 처리
- Sheet 숨기기 처리
- 행/열 숨기기
- Sheet 보호 처리
- 함수 치환 처리
- 외부파일 참조
- 메모에 “개인정보” 입력
- “개인정보”가 포함된 개체 삽입 (OLE개체)

2. 개인정보가 포함된 첨부파일 게시< ①이미지 파일 노출 >

첨부된 이미지 파일(PDF, JPG 등)에 개인정보 포함

노출사례

- 이미지 파일 첨부를 통한 개인정보 노출

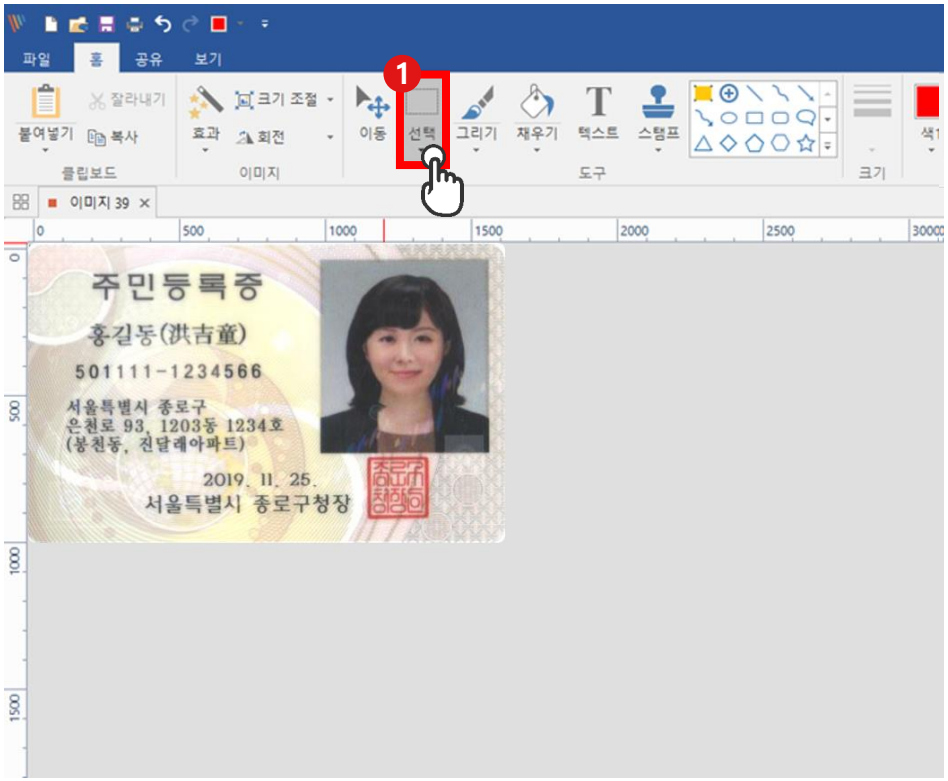


2. 개인정보가 포함된 첨부파일 게시< ①이미지 파일 노출 >

첨부된 이미지 파일(PDF, JPG 등)에 개인정보 포함

조치방법

- 이미지 편집 소프트웨어 등을 이용해 개인정보 마스킹 처리

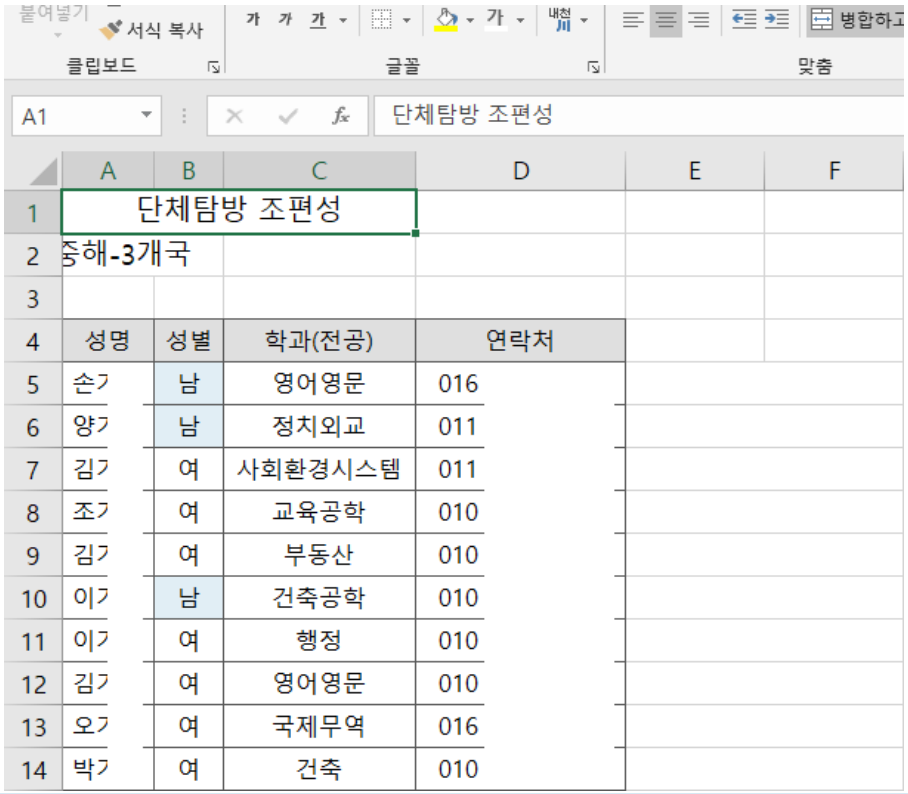


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

배경색과 글자색 동일

노출사례

- 배경색과 동일하게 설정된 글자색으로 인한 개인정보 노출



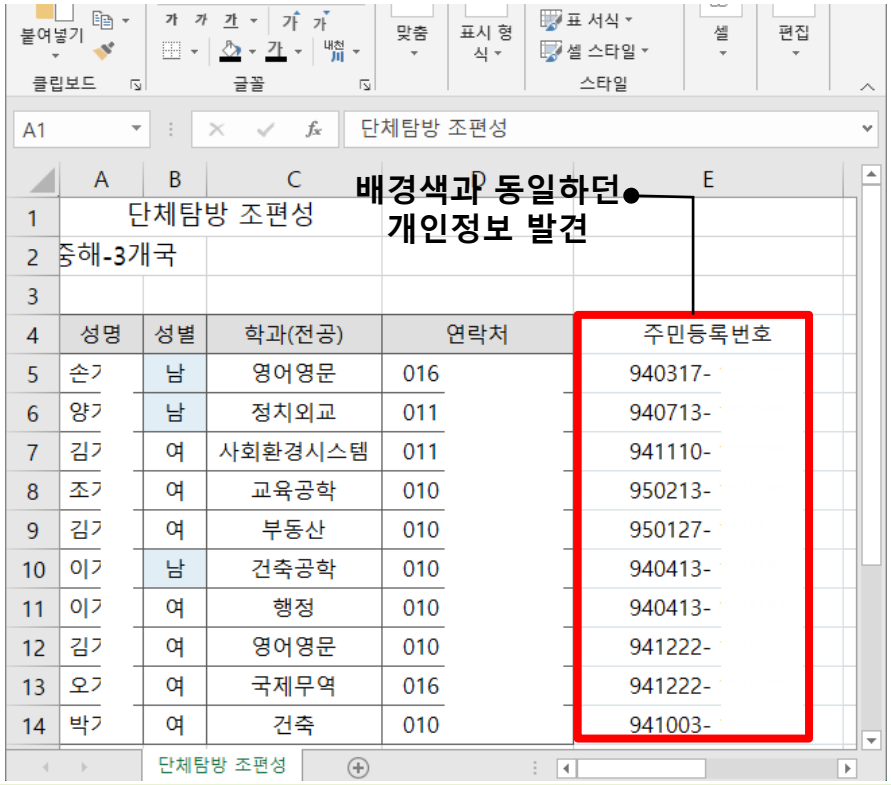
	A	B	C	D	E	F
1	단체탐방 조편성					
2	중해-3개국					
3						
4	성명	성별	학과(전공)	연락처		
5	손기	남	영어영문	016		
6	양기	남	정치외교	011		
7	김기	여	사회환경시스템	011		
8	조기	여	교육공학	010		
9	김기	여	부동산	010		
10	이기	남	건축공학	010		
11	이기	여	행정	010		
12	김기	여	영어영문	010		
13	오기	여	국제무역	016		
14	박기	여	건축	010		

2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

배경색과 글자색 동일

조치방법(1)

- 셀 전체 선택 후 배경색 채우기 없음 및 글자 색 변경
- 나타난 개인정보 삭제 또는 마스킹

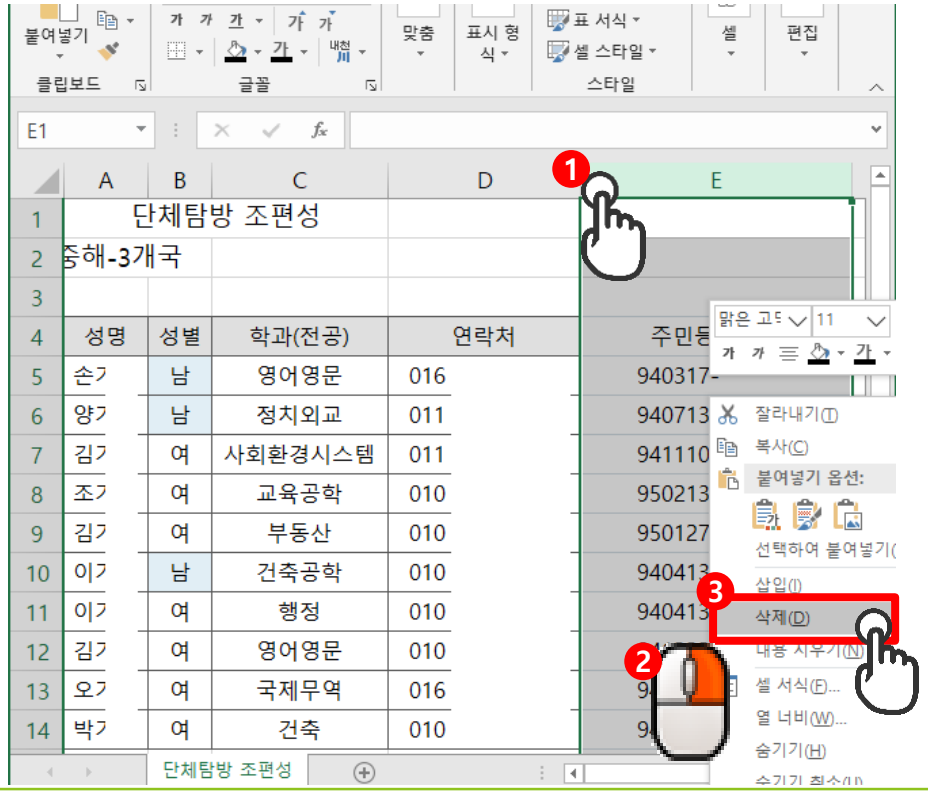


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

배경색과 글자색 동일

조치방법(2)

- 글자 색 변경 후 나타난 노출된 개인정보 삭제 또는 마스킹

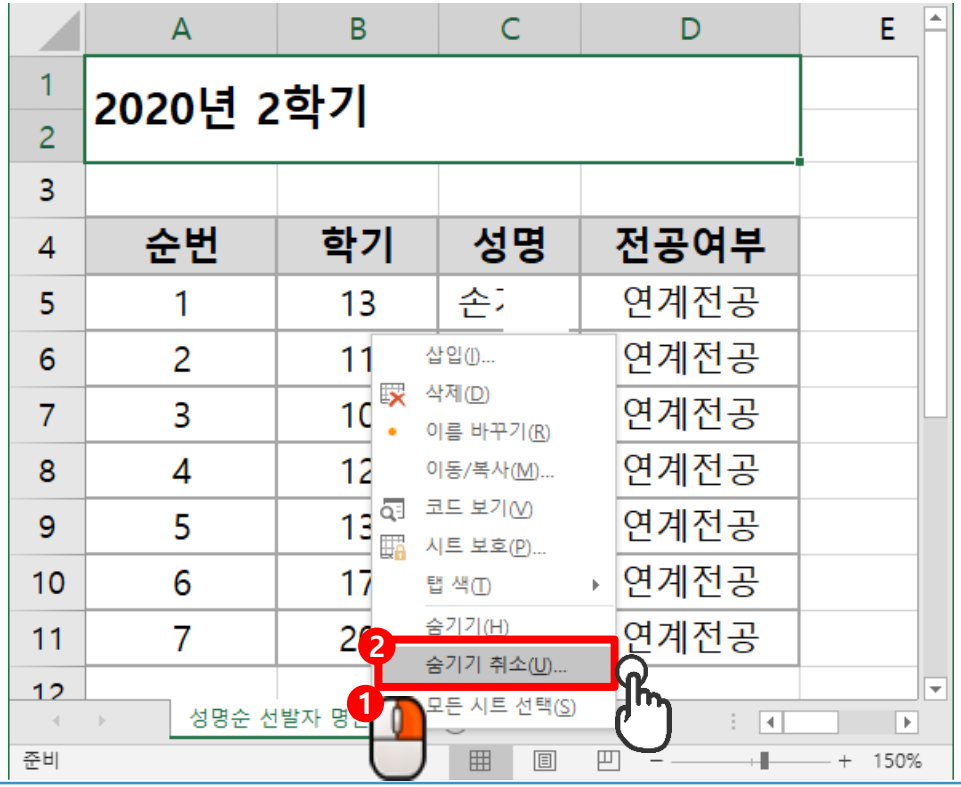


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

Sheet[숨기기] 처리

노출사례

- Sheet 숨기기 취소 후 나타난 개인정보

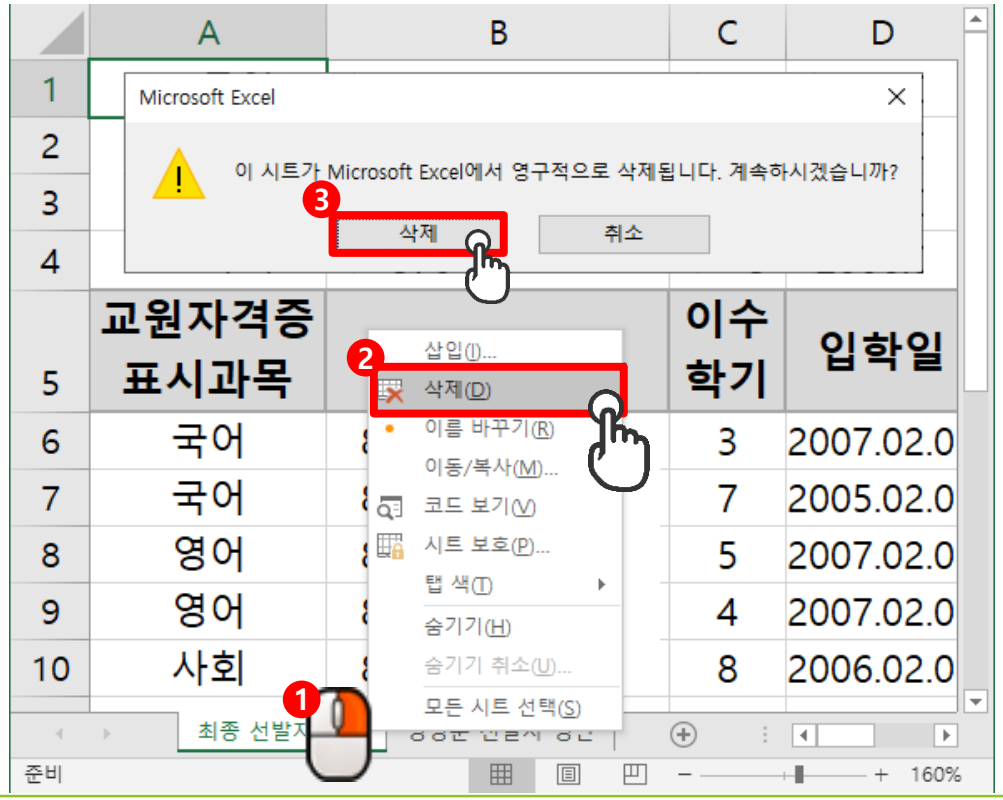


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

Sheet[숨기기] 처리

조치방법

- 숨기기 처리된 Sheet 삭제 조치

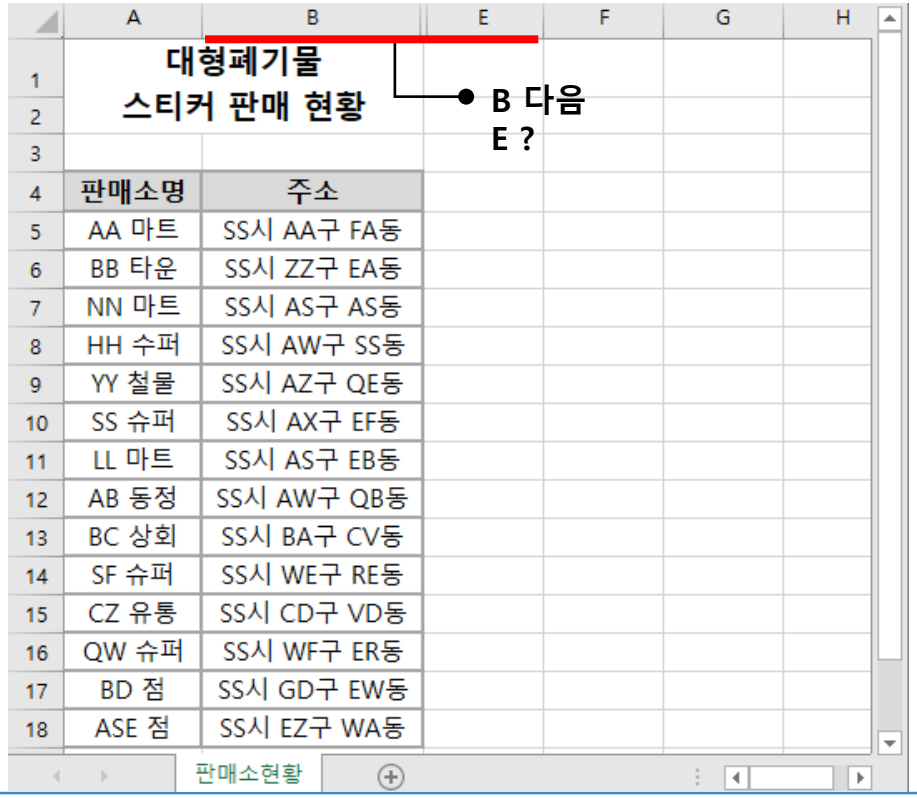


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

행/열[숨기기] 처리

노출사례

- 행/열 숨기기 취소로 노출되는 개인정보



2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

행/열[숨기기] 처리

조치방법

- 숨기기 처리된 행/열 삭제 또는 마스킹 처리

	A	B	C	D	E
1	대형폐기물 스티커 판매 현황				
2					
3					
4	판매소명	주소	대표자명	주민등록번호	
5	AA 마트	SS시 AA구 FA동	조가식	440227-[redacted]	
6	BB 타운	SS시 ZZ구 EA동	조가숙	621013-[redacted]	
7	NN 마트	SS시 AS구 AS동	김가숙	561230-[redacted]	
8	HH 수퍼	SS시 AW구 SS동	이가숙	550424-[redacted]	
9	YY 철물	SS시 AZ구 QE동	이가호	780822-[redacted]	
10	SS 슈퍼	SS시 AX구 EF동	조기자	630417-[redacted]	
11	LL 마트	SS시 AS구 EB동	유가령	691110-[redacted]	
12	AB 동정	SS시 AW구 QB동	남기훈	750126-[redacted]	
13	BC 상회	SS시 BA구 CV동	김가자	741231-[redacted]	
14	SF 슈퍼	SS시 WE구 RE동	이기태	640717-[redacted]	
15	CZ 유통	SS시 CD구 VD동	이기창	590923-[redacted]	
16	QW 슈퍼	SS시 WF구 ER동	오가융	870402-[redacted]	
17	BD 점	SS시 GD구 EW동	김기수	750125-[redacted]	
18	ASE 점	SS시 EZ구 WA동	광기수	660522-[redacted]	

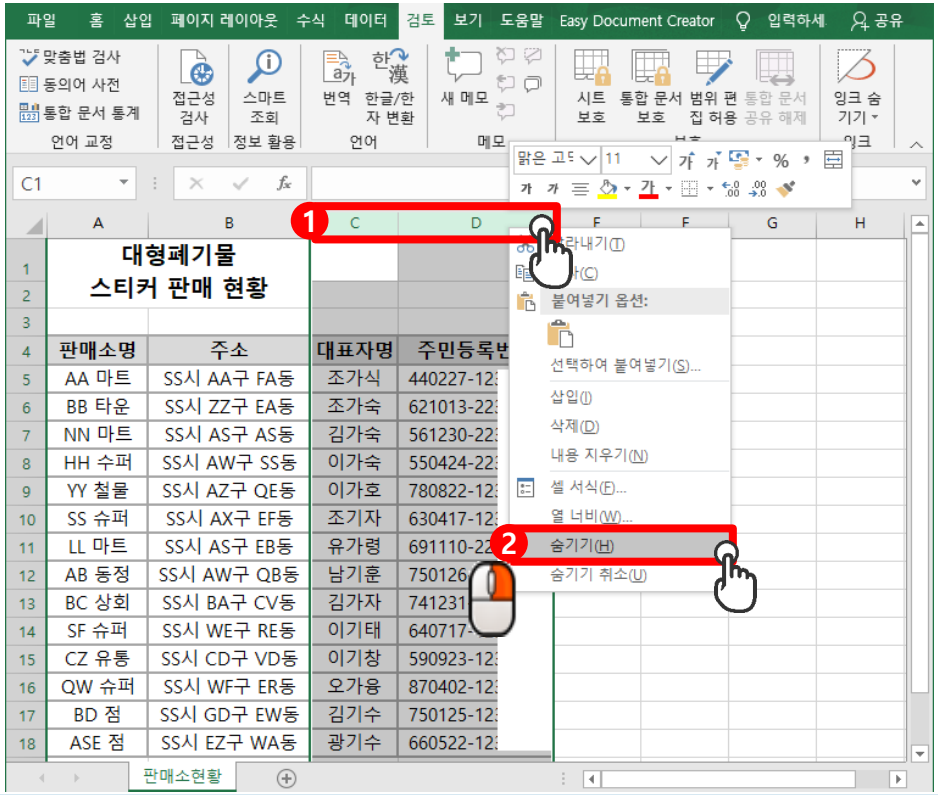
판매소현황

2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

Sheet 보호 처리

노출사례(1)

- 시트보호로 개인정보가 보호되지 않는 사례
  - 개인정보 숨김 처리 후 시트보호 및 통합 문서 보호

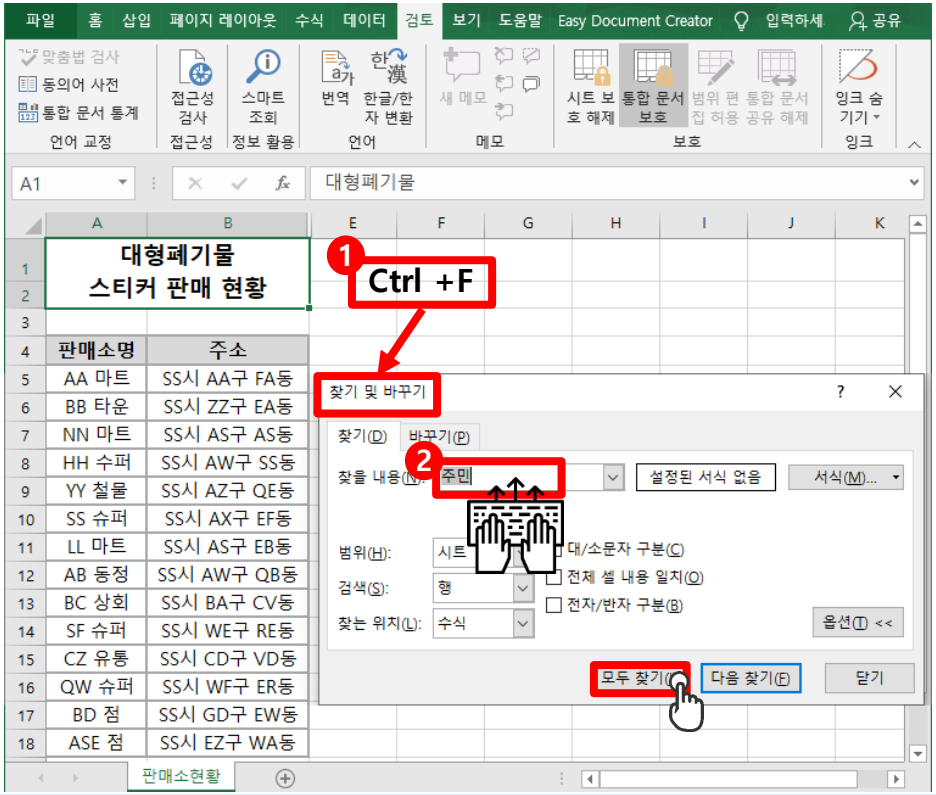


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

Sheet 보호 처리

노출사례(2)

- 시트보호로 개인정보가 보호되지 않는 사례
  - 찾기 및 바꾸기 기능으로 개인정보 노출

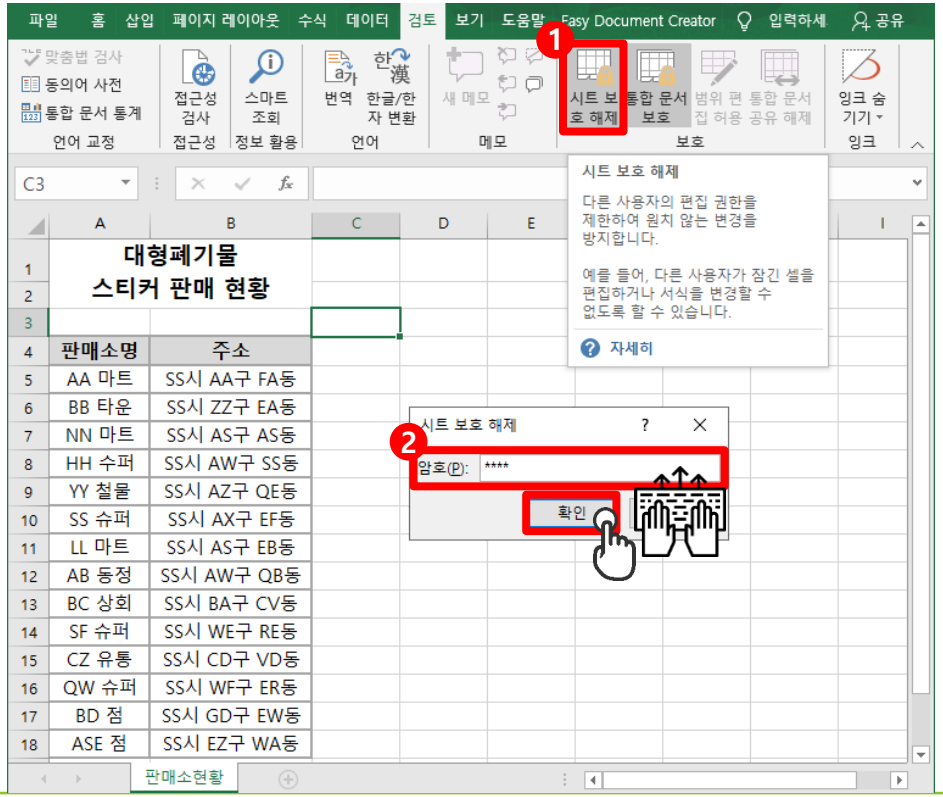


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

Sheet 보호 처리

조치방법(1)

- 시트보호 해제 및 개인정보 삭제 또는 마스킹

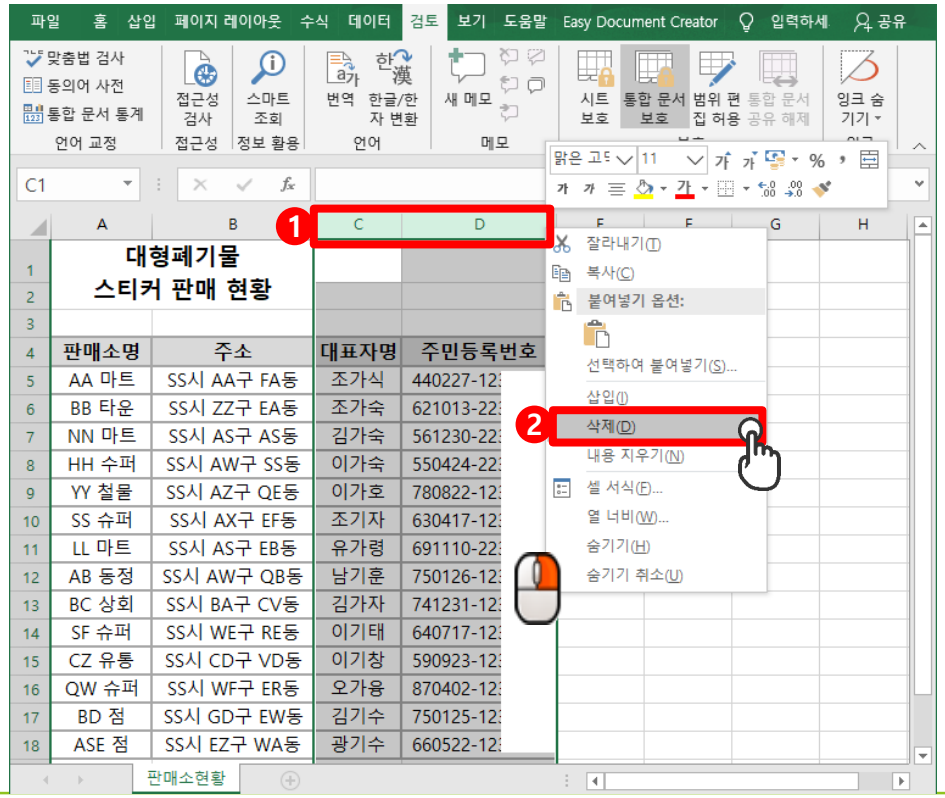


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

Sheet 보호 처리

조치방법(2)

- 시트보호 해제 및 개인정보 삭제 또는 마스킹



2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

치환 함수

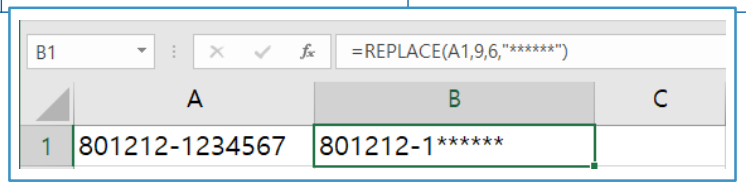
노출사례(1)

- 치환 함수 및 행/열 숨김으로 인한 노출사례

함수명	사용함수	기존값	결과값
REPLACE	=REPLACE(A1,9,6,"******")	801212-1234567	801212-1******
SUBSTITUTE	=SUBSTITUTE(A1,"234567","******")	801212-1234567	801212-1******
LEFT	=LEFT(A1,8)&"******"	801212-1234567	801212-1******

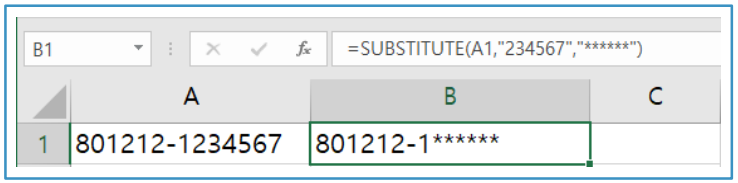
REPLACE

텍스트의 일부를
다른 텍스트로 치환



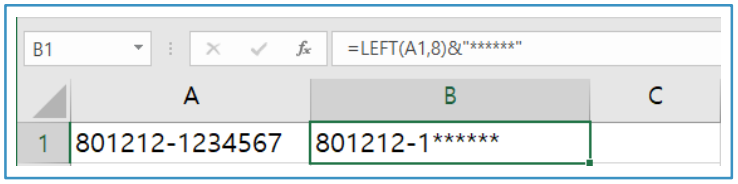
SUBSTITUTE

텍스트 중의 old_text를 찾아서
원하는 new_text로 변경



LEFT

텍스트 문자열의 시작 지점부터
지정한 수만큼의 문자를 반환

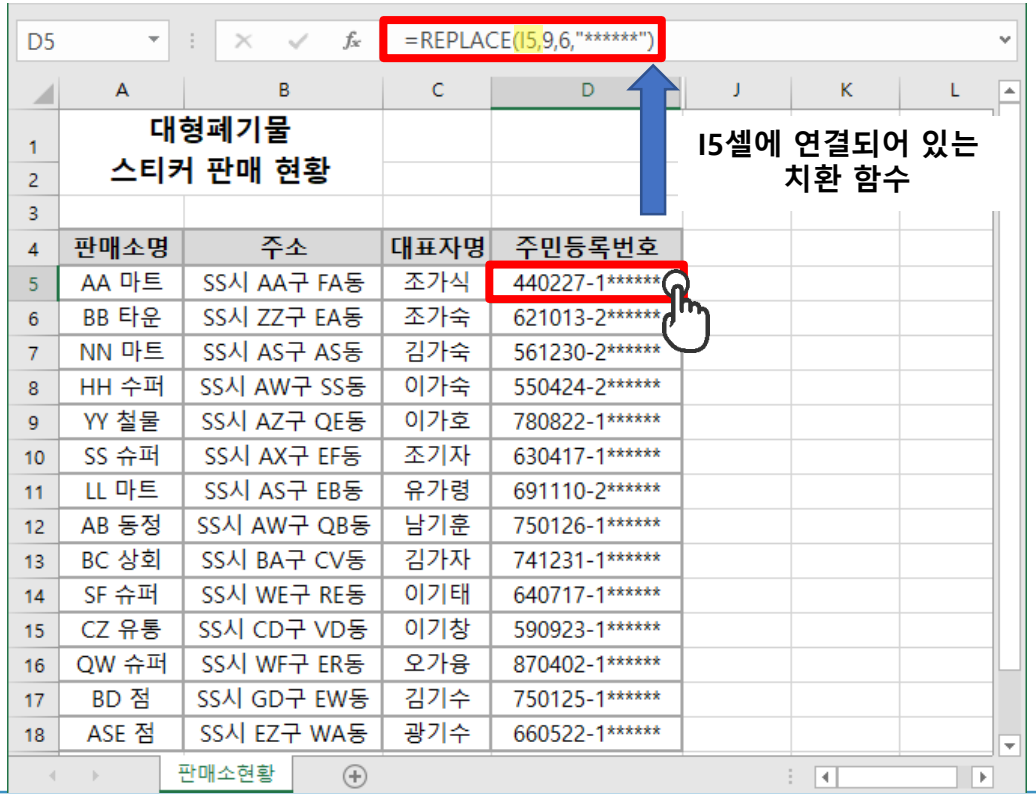


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

치환 함수

노출사례(2)

- 치환함수로 마스킹 처리된 필드를 해제/취소한 경우 노출

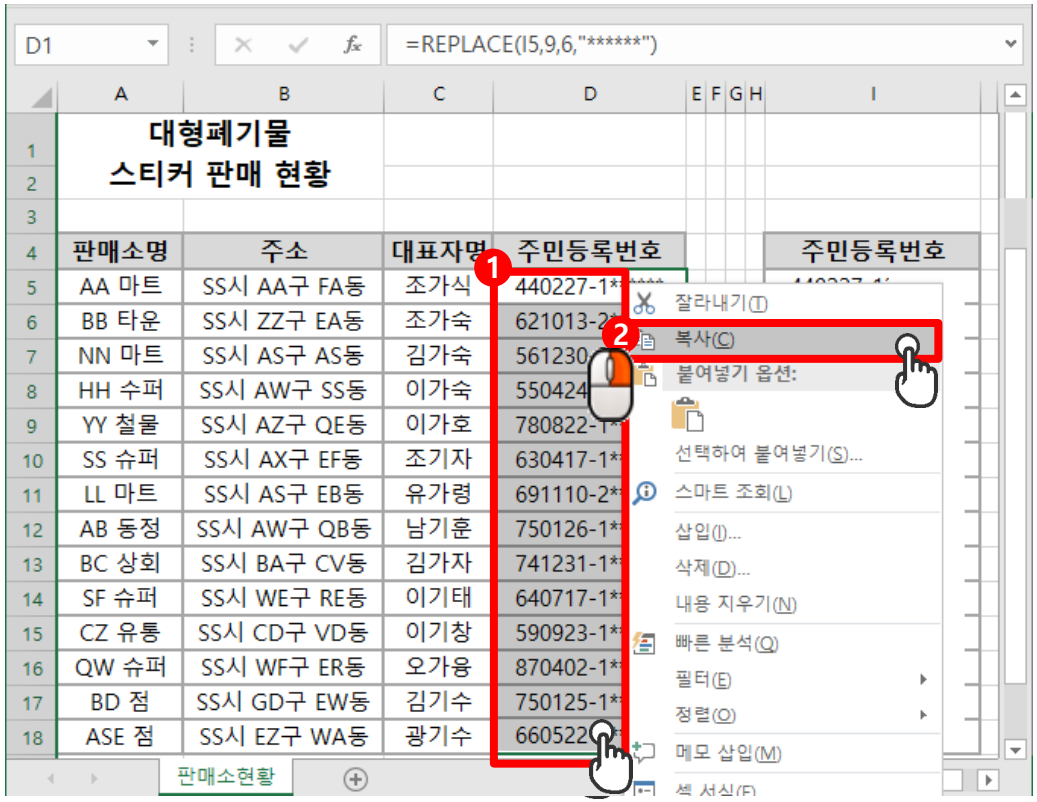


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

치환 함수

조치방법(1)

- 치환함수가 들어있는 행/열 복사 및 '값' 붙여넣기

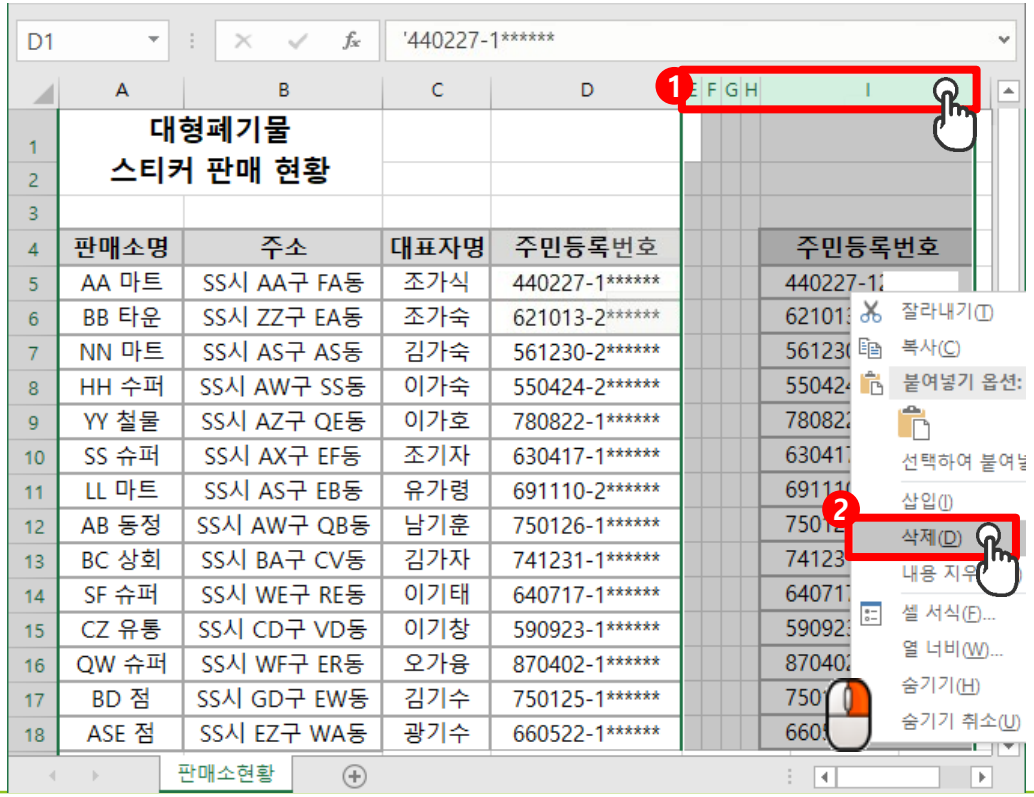


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

치환 함수

조치방법(2)

- 원본 행/열 삭제 및 연결된 값 확인

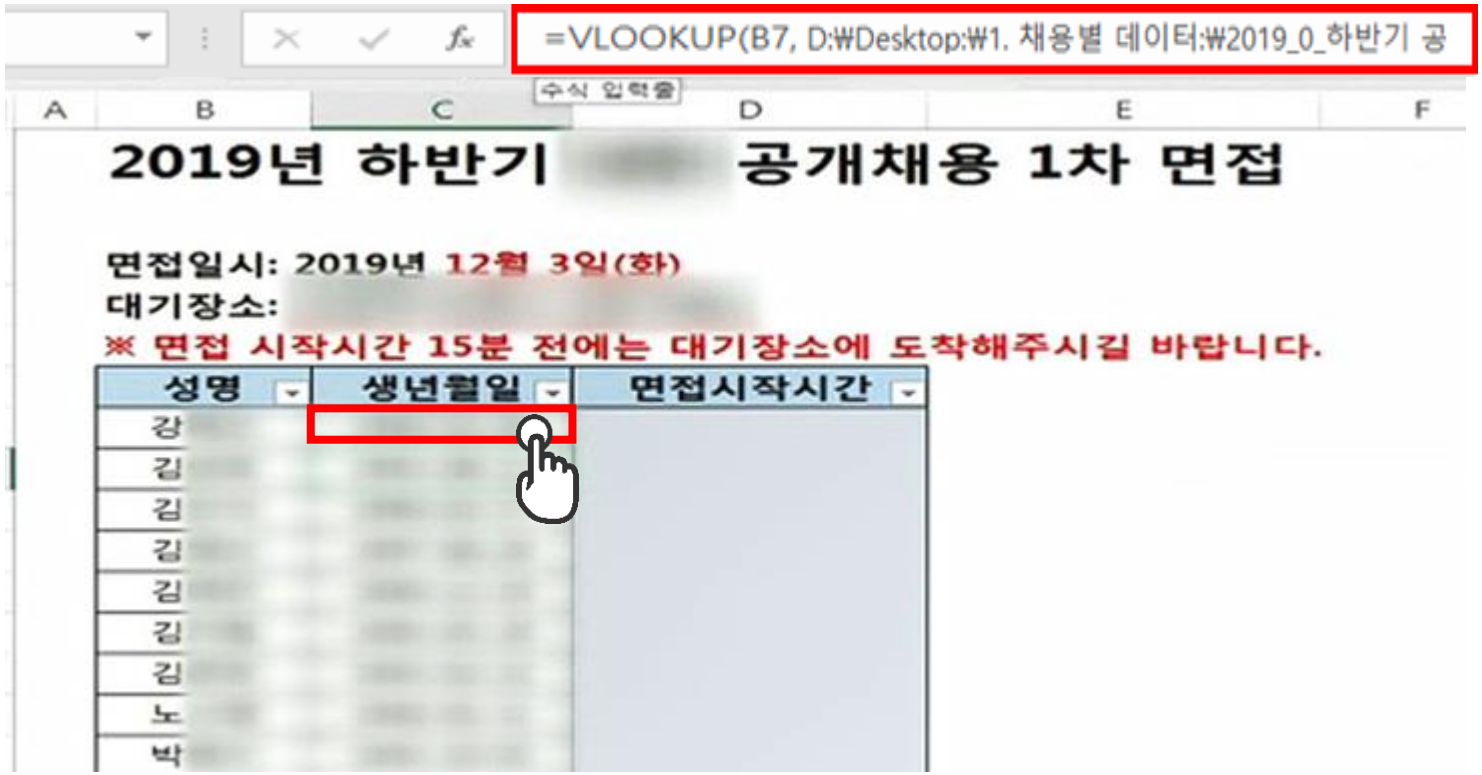


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

노출사례(1)

- 외부파일 참조 기능으로 개인정보 노출
  - 외부파일 참조 수식을 이용한 함수

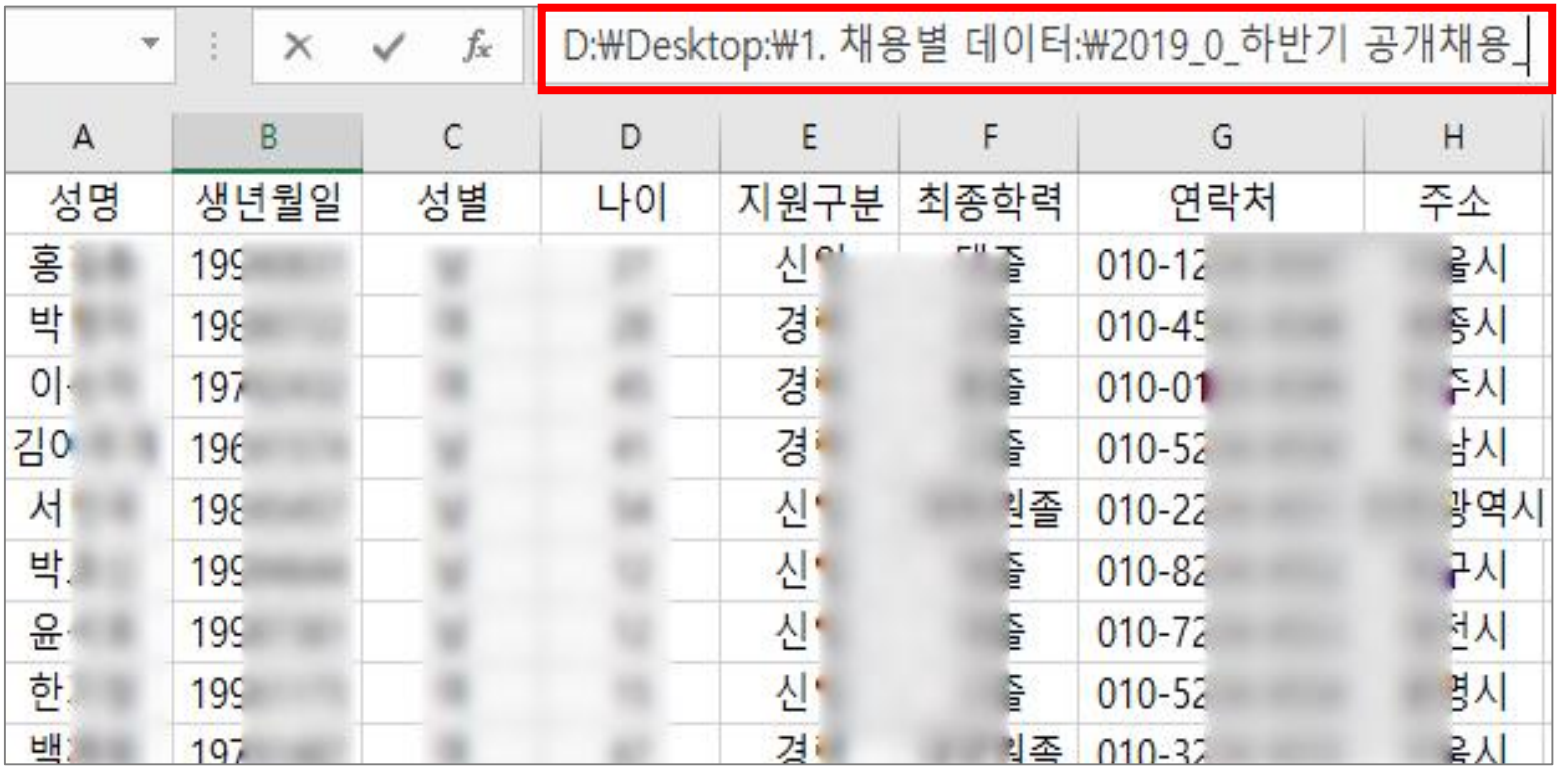


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

노출사례(2)

- 외부파일 참조 기능으로 개인정보 노출
  - 외부파일 연결값 저장으로 인한 노출



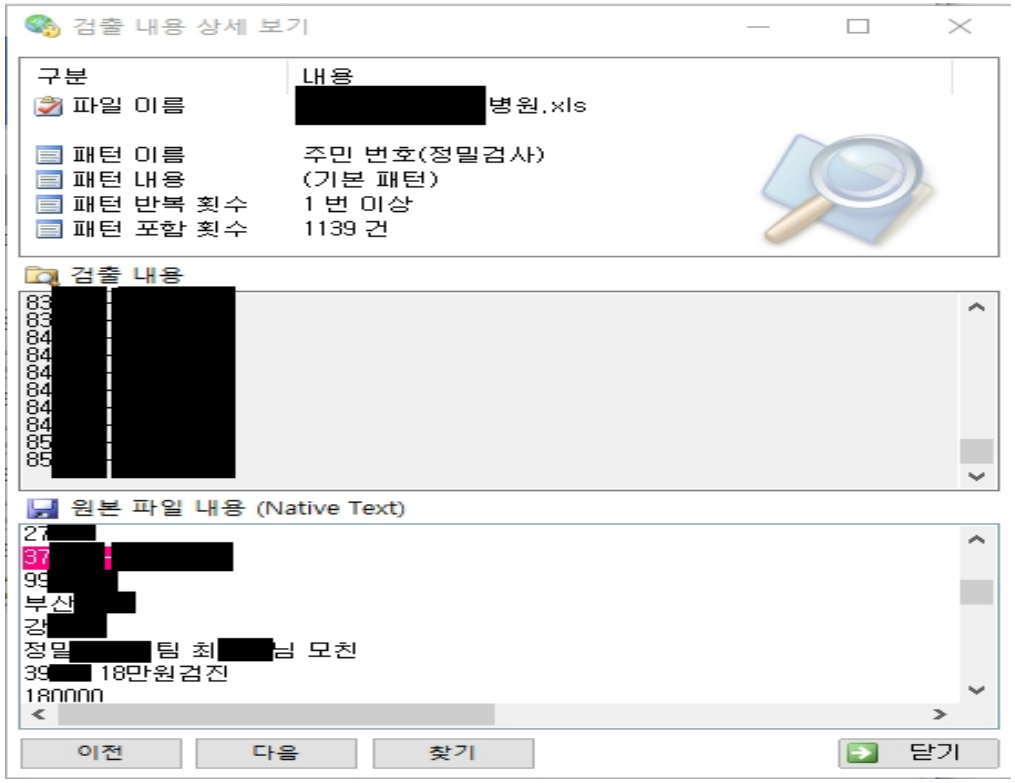
A	B	C	D	E	F	G	H
성명	생년월일	성별	나이	지원구분	최종학력	연락처	주소
홍	199			신	대졸	010-12	울시
박	198			경	졸	010-45	동시
이	197			경	졸	010-01	주시
김0	196			경	졸	010-52	남시
서	198			신	원졸	010-22	광역시
박	199			신	졸	010-82	구시
윤	199			신	졸	010-72	전시
한	199			신	졸	010-52	명시
백	197			경	원졸	010-32	울시

2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

노출사례(3)

- 개인정보 탐지 솔루션을 통한 노출

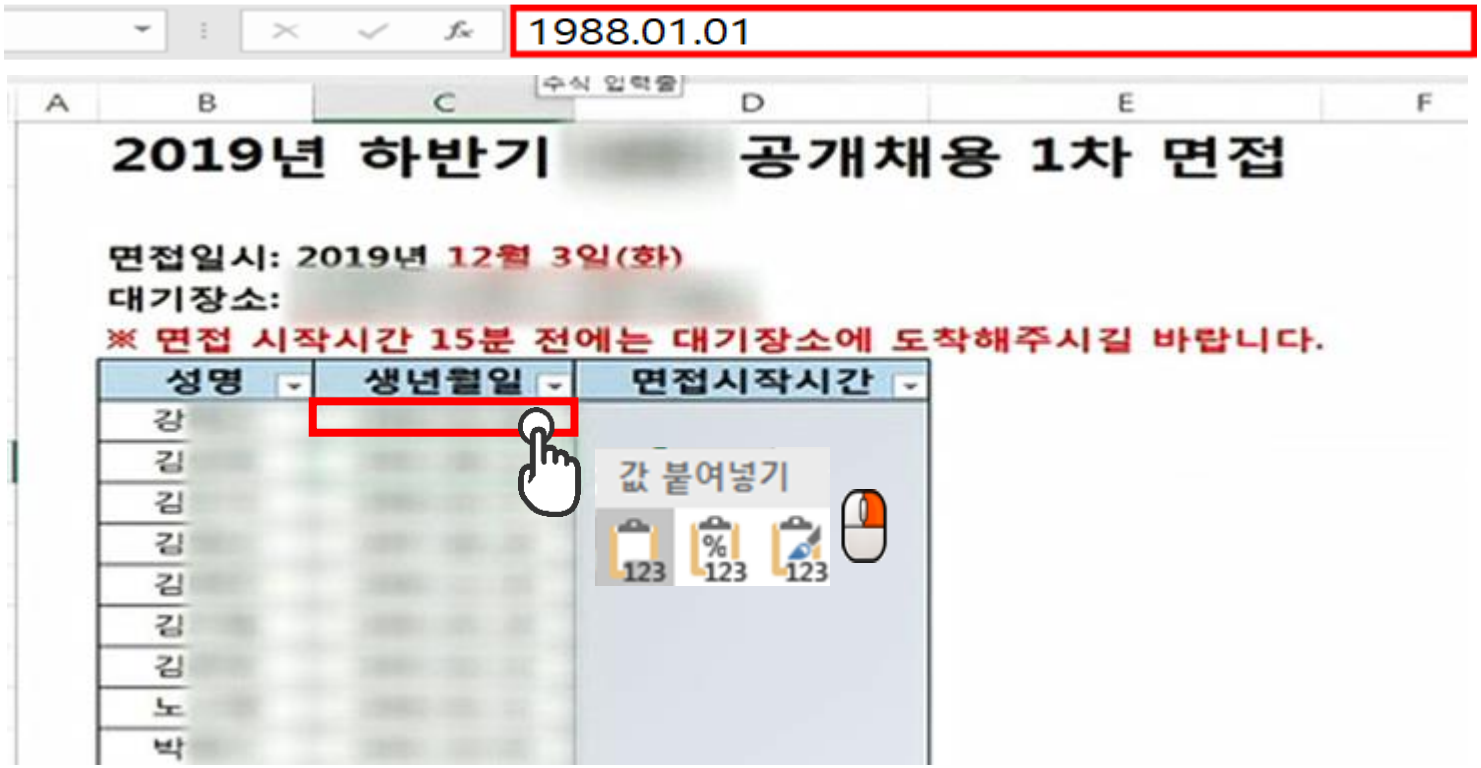


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

조치방법(1)

- 외부파일 연결 시, 값 붙여넣기 및 불필요한 개인정보 마스킹



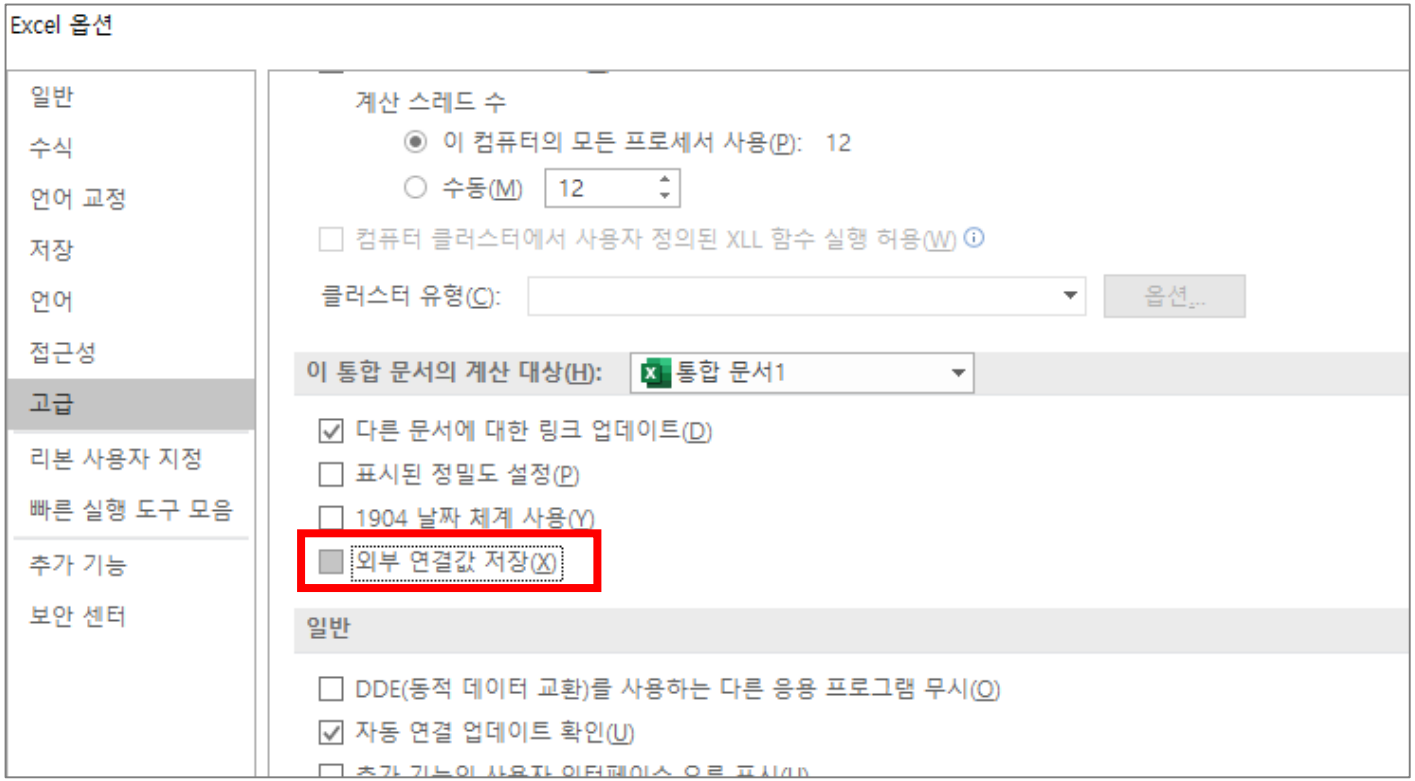
2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

조치방법(2)

- 엑셀 고급 옵션 중 '외부 연결값 저장' 기능 체크박스 해제

※ 파일 → 옵션 → 고급 → 외부 연결값 저장 체크박스 해제

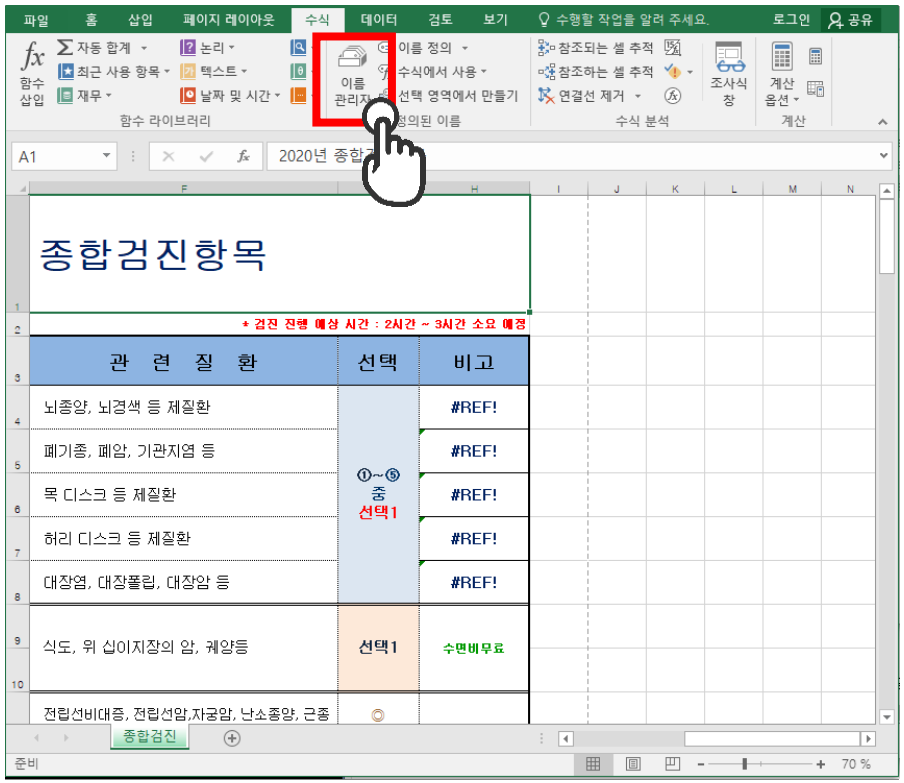


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

조치방법(3)

- 수식 메뉴 '이름 관리자' 내 리스트 삭제

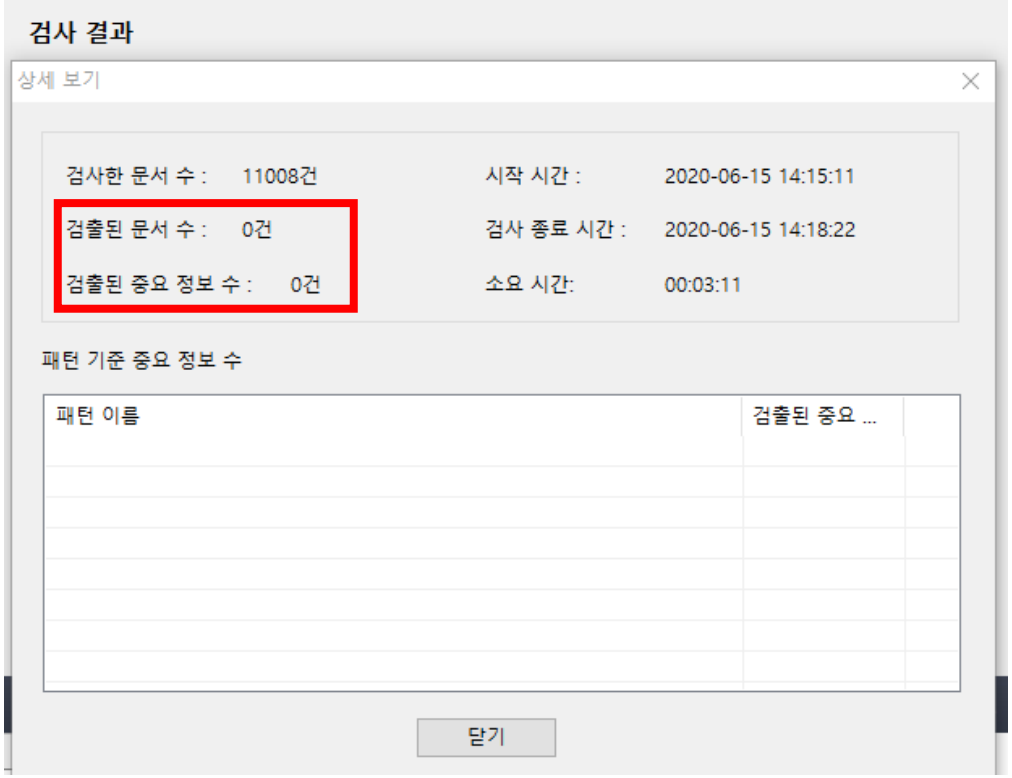


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

외부파일 참조

조치방법(4)

- 개인정보 탐지 솔루션을 통한 노출 여부 재확인

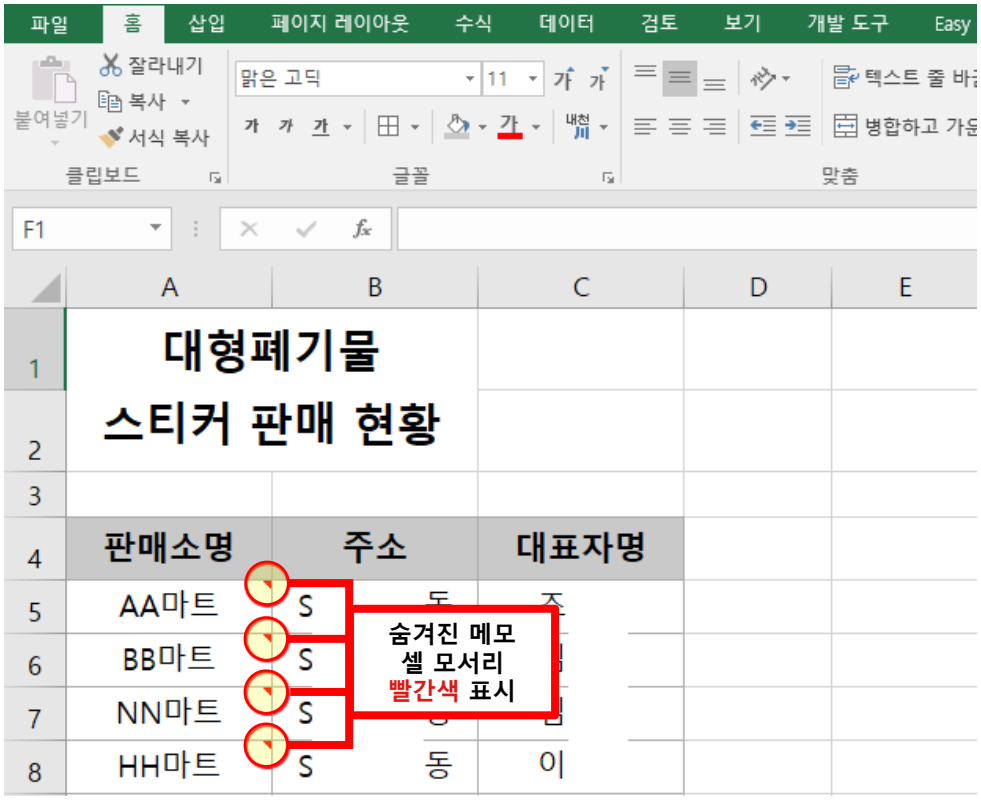


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

메모

노출사례

- 메모 삽입 여부 확인
  - 정보확인, 검토 기능 확인

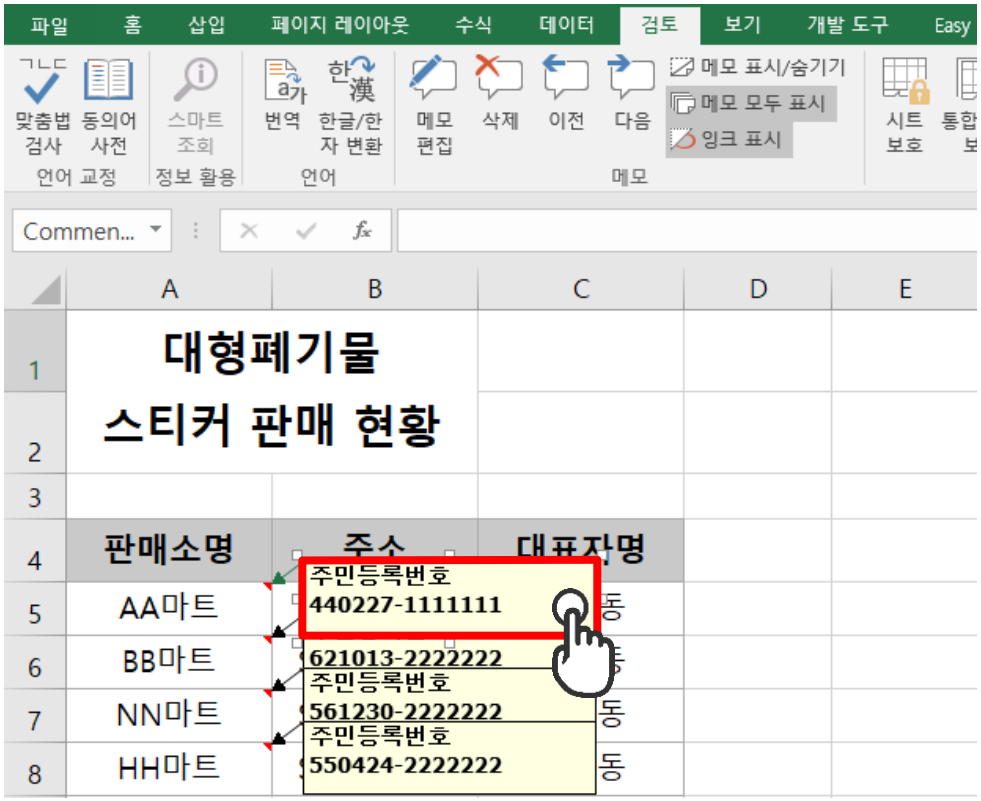


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

메모

조치방법

- 메모에 기록된 개인정보 삭제 또는 마스킹
  - 메모 선택 후 삭제 또는 편집 / 메모 표시 탭의 비활성화 확인

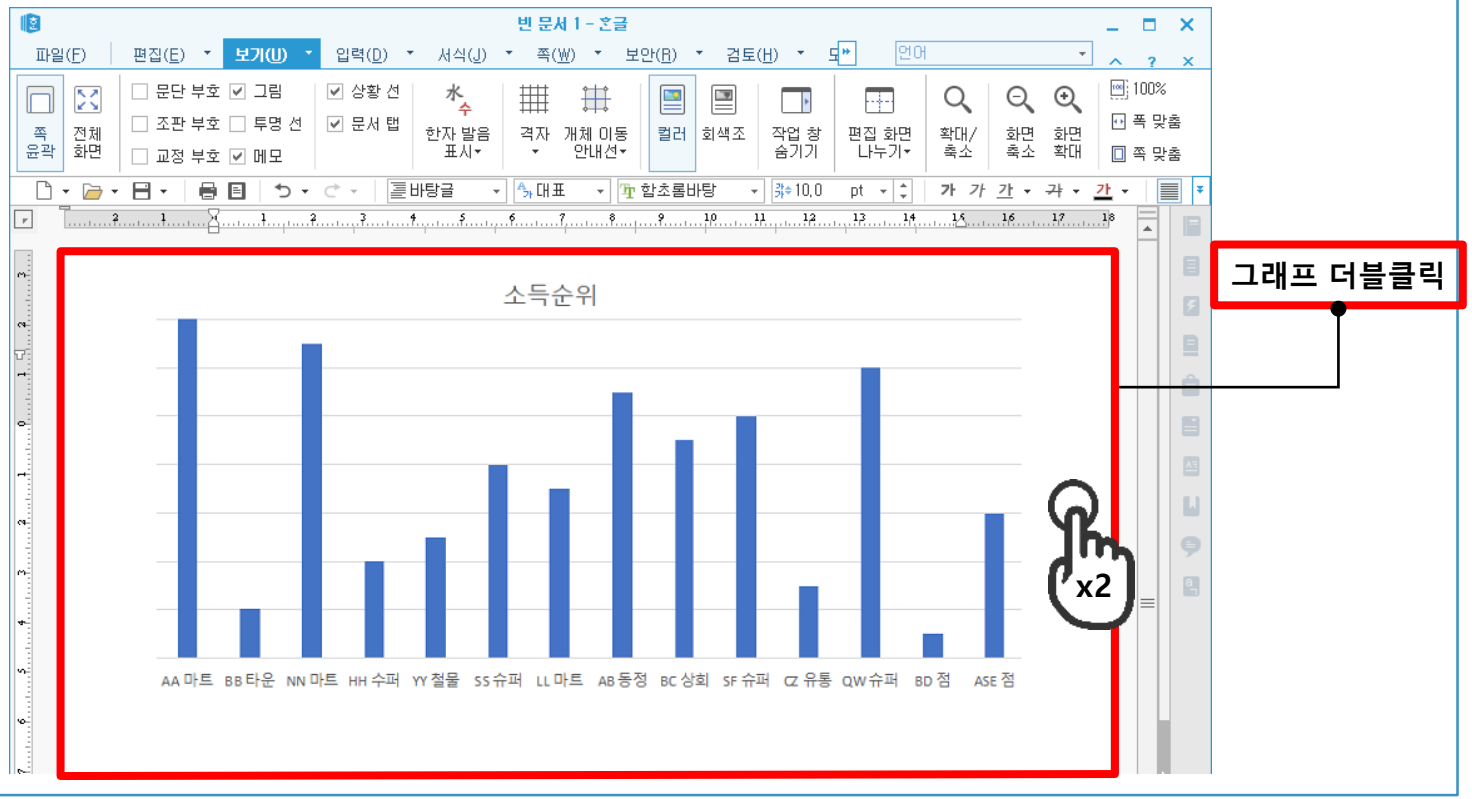


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

객체(OLE) 삽입

노출사례

- OLE 객체에 포함되어 있던 개인정보 노출

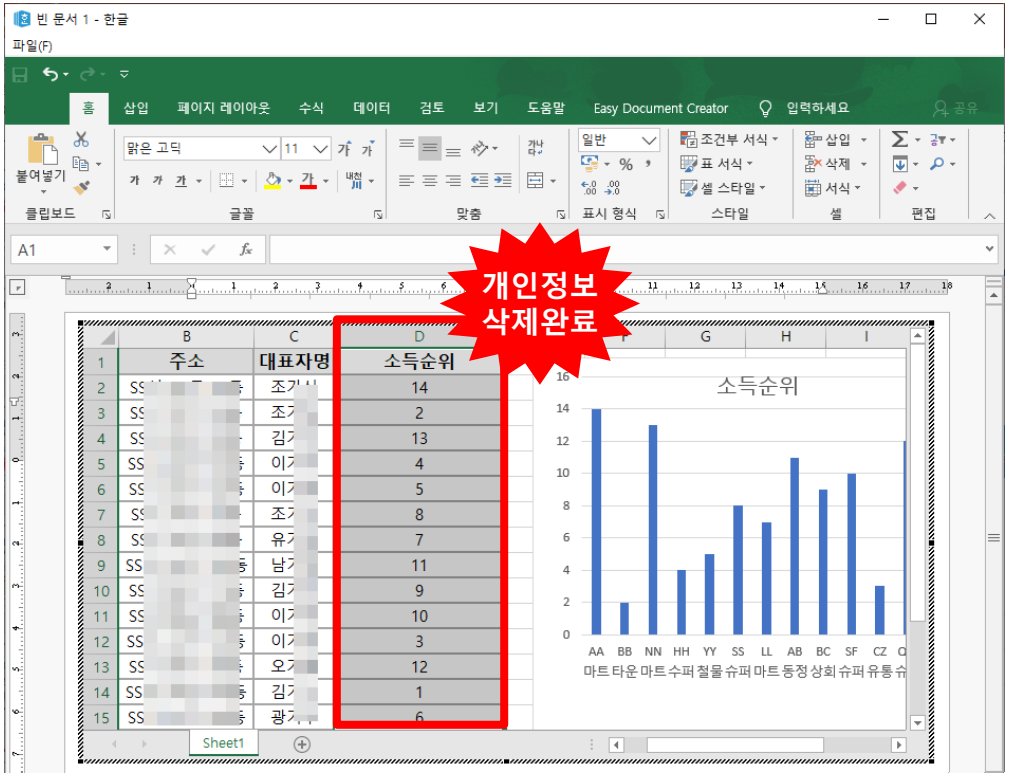


2. 개인정보가 포함된 첨부파일 게시< ②엑셀 파일 노출 >

객체(OLE) 삽입

조치방법

- OLE 객체에 포함된 엑셀시트 개인정보 삭제 또는 마스킹

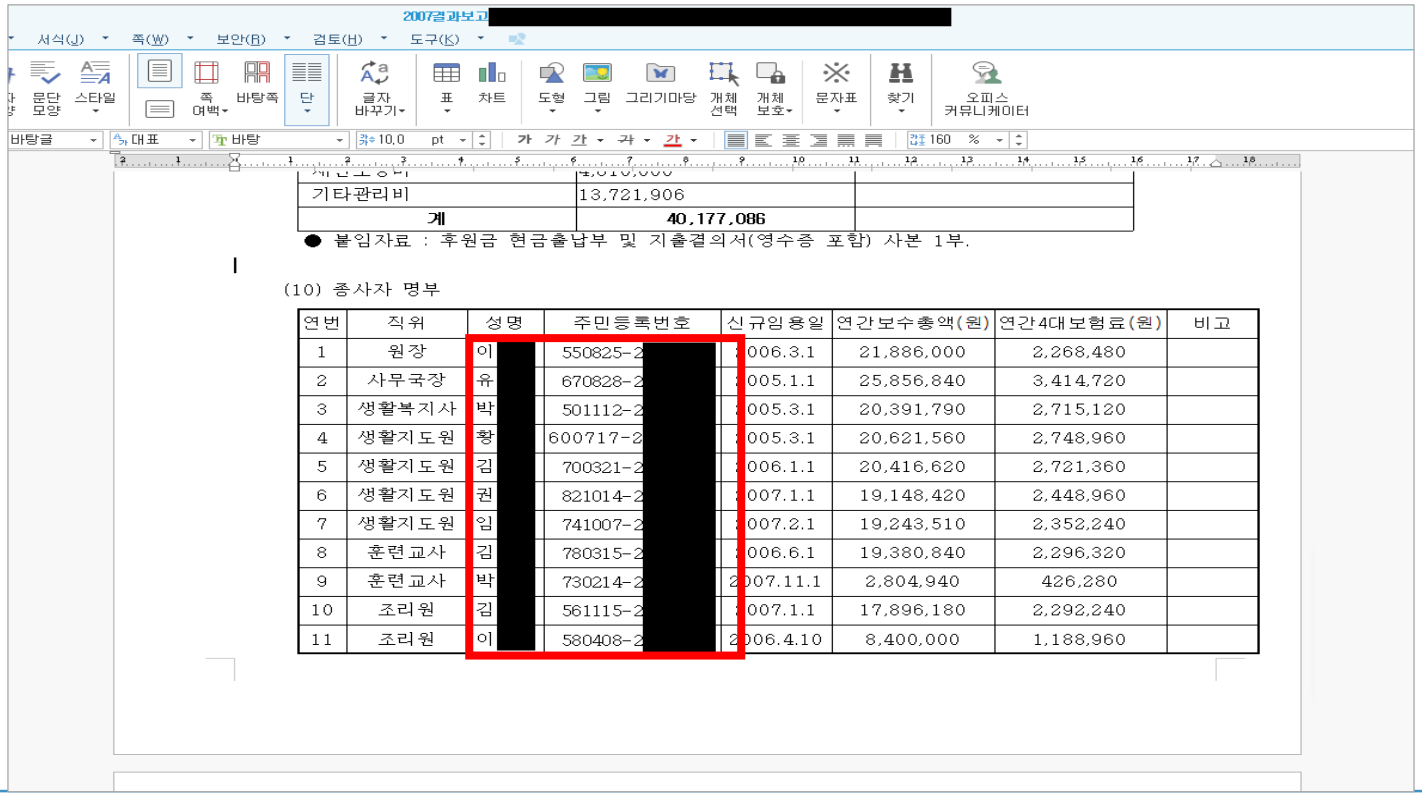


2. 개인정보가 포함된 첨부파일 게시 < ③한글파일 노출 >

첨부된 한글파일(HWP, DOC)에 개인정보 노출

노출사례

- 개인정보가 포함된 한글문서



기타관리비	13,721,906	
계	40,177,086	

● 붙임자료 : 후원금 현금출납부 및 지출결의서(영수증 포함) 사본 1부.

(10) 종사자 명부

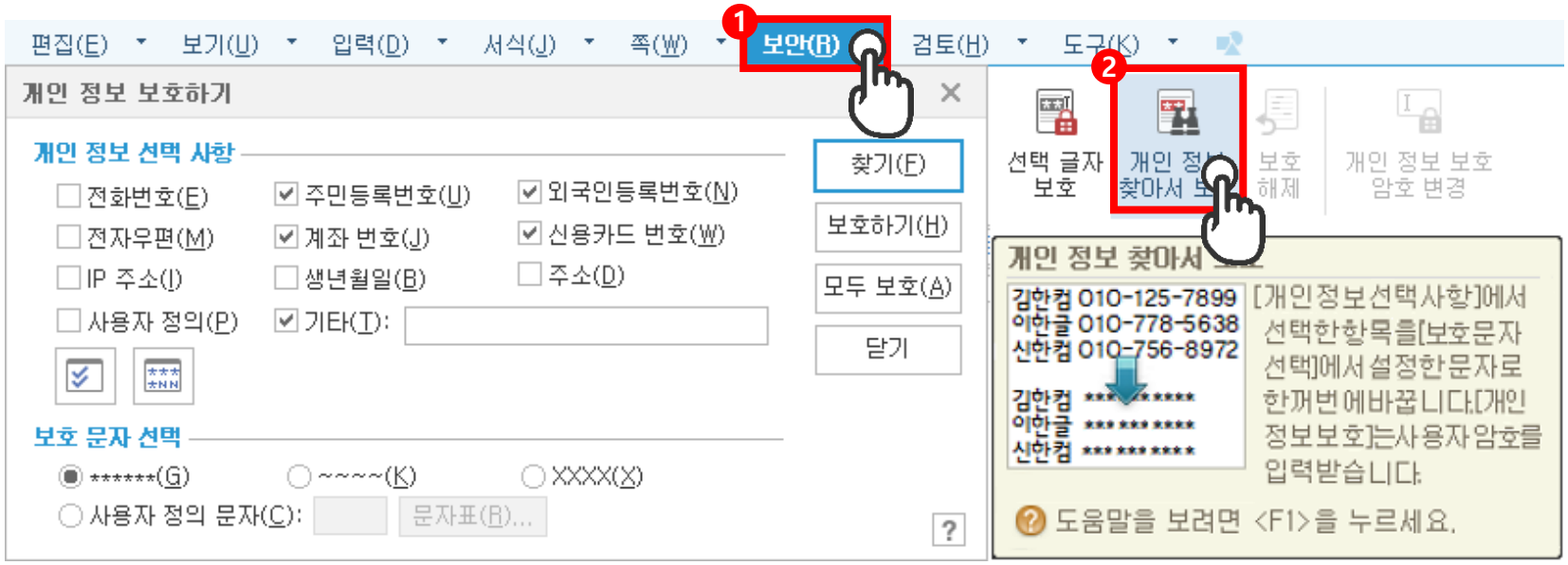
연번	직위	성명	주민등록번호	신규임용일	연간보수총액(원)	연간4대보험료(원)	비고
1	원장	이[redacted]	550825-2[redacted]	2006.3.1	21,886,000	2,268,480	
2	사무국장	유[redacted]	670828-2[redacted]	2005.1.1	25,856,840	3,414,720	
3	생활복지사	박[redacted]	501112-2[redacted]	2005.3.1	20,391,790	2,715,120	
4	생활지도원	황[redacted]	600717-2[redacted]	2005.3.1	20,621,560	2,748,960	
5	생활지도원	김[redacted]	700321-2[redacted]	2006.1.1	20,416,620	2,721,360	
6	생활지도원	권[redacted]	821014-2[redacted]	2007.1.1	19,148,420	2,448,960	
7	생활지도원	임[redacted]	741007-2[redacted]	2007.2.1	19,243,510	2,352,240	
8	훈련교사	김[redacted]	780315-2[redacted]	2006.6.1	19,380,840	2,296,320	
9	훈련교사	박[redacted]	730214-2[redacted]	2007.11.1	2,804,940	426,280	
10	조리원	김[redacted]	561115-2[redacted]	2007.1.1	17,896,180	2,292,240	
11	조리원	이[redacted]	580408-2[redacted]	2006.4.10	8,400,000	1,188,960	

2. 개인정보가 포함된 첨부파일 게시 < ③한글파일 노출 >

첨부된 한글파일(HWP, DOC)에 개인정보 노출

조치방법(1)

- 한글의 개인정보 보호 기능 이용

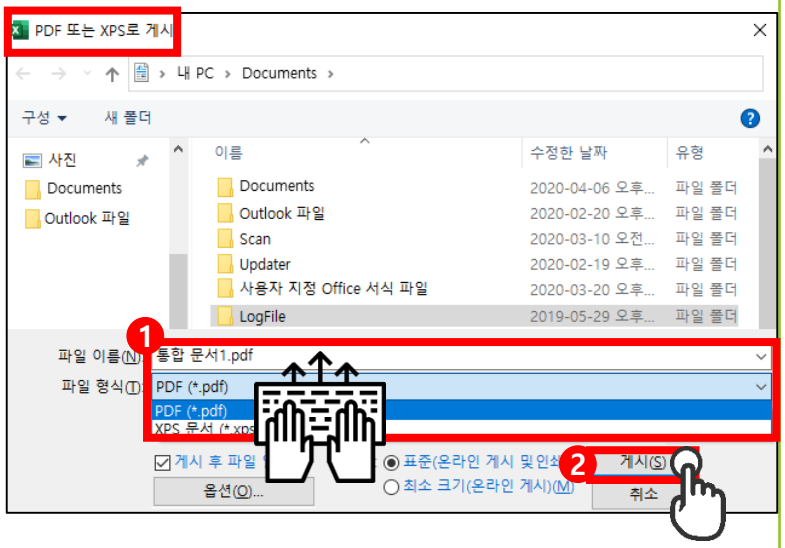


[참고] PDF 파일 내보내기

이용자 공지 등의 용도일 경우, PDF로 변환하여 활용 권장

조치방법(2)

- 내보내기를 이용하여 엑셀을 PDF로 변환하여 사용

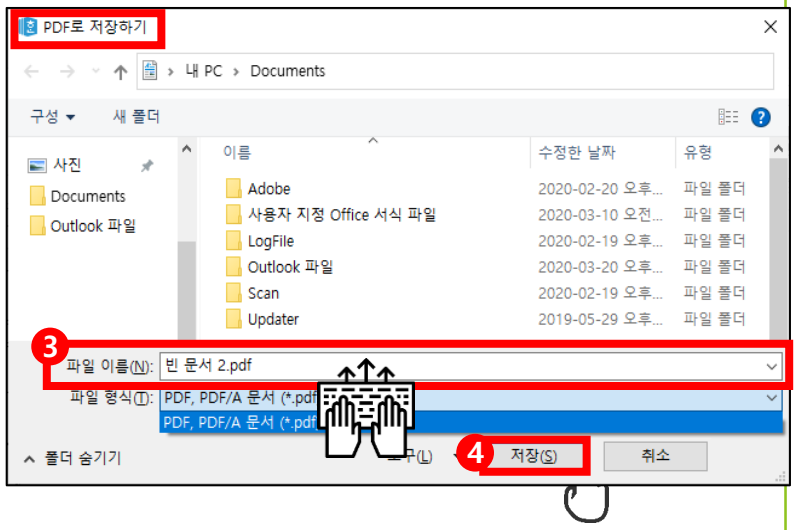


[참고] PDF 파일 내보내기

이용자 공지 등의 용도일 경우, PDF로 변환하여 활용 권장

조치방법(3)

- 한글 저장 시 PDF로 저장하기를 선택해 변환해서 사용



개인정보 노출사례 ②

홈페이지 이용자 부주의

1. 게시글 및 첨부파일에 개인정보 노출

이용자가 문의 글 등을 게시하며 개인정보 노출

노출사례

- **게시글 및 첨부파일에 의한 개인정보 노출**

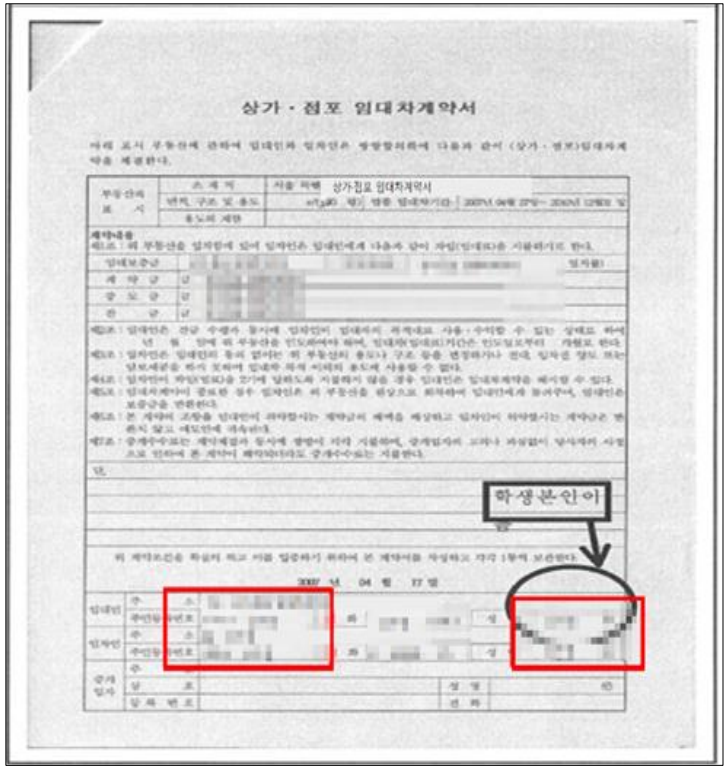
[항공권 구매기록] 문의

작성자 [redacted]

안녕하세요.

항공사 마일리지 적립을 위하여 다음과 같은 사항 요청 드립니다.

* 탑승자명 : [redacted]
* 여권번호 : [redacted]
* 요청사항 : 2015년~2016년의 항공권 구매기록 및 티켓번호
* 연락처 : 010-[redacted]

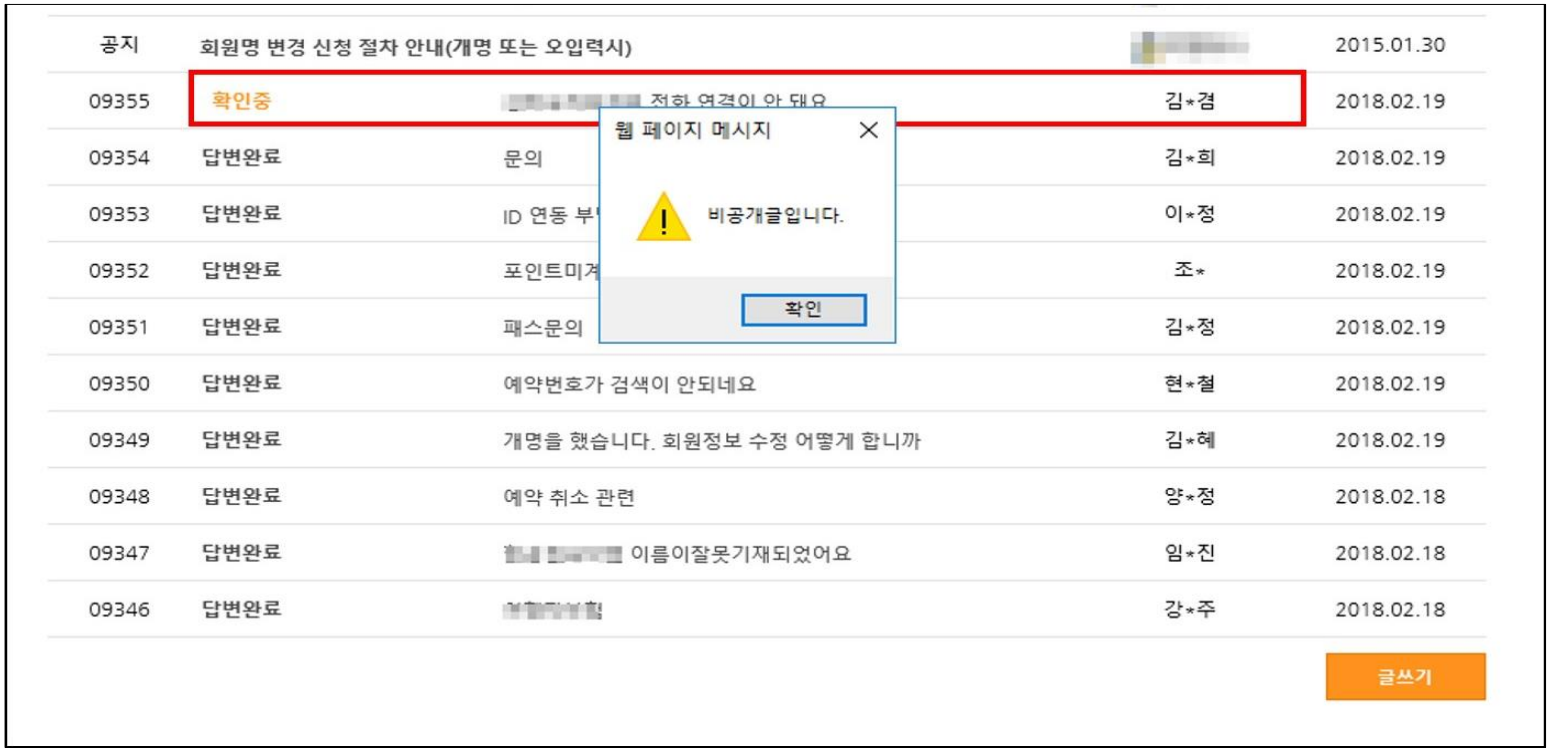


1. 게시글 및 첨부파일에 개인정보 노출

이용자가 문의 글 등을 게시하며 개인정보 노출

조치방법(1)

- 게시물 비공개 전환 또는 개인정보 삭제

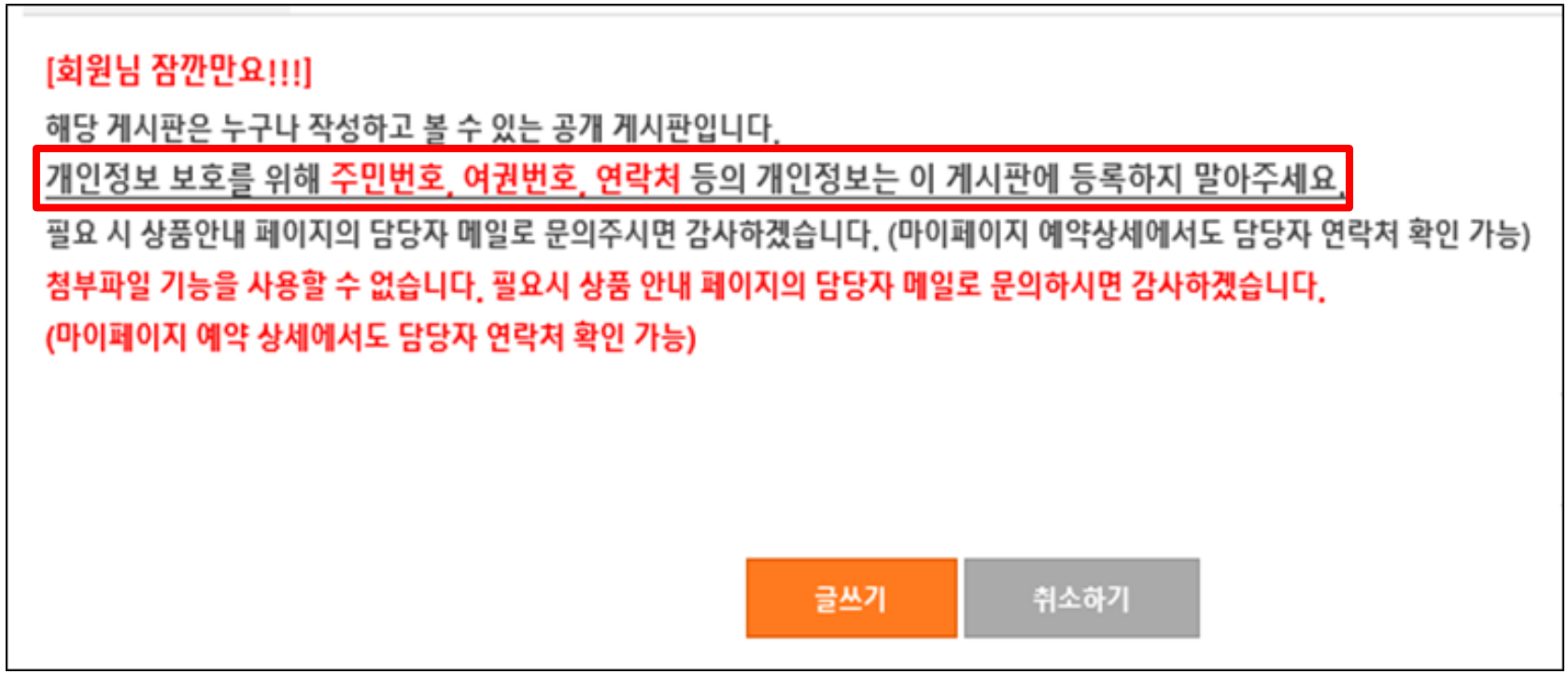


1. 게시글 및 첨부파일에 개인정보 노출

이용자가 문의 글 등을 게시하며 개인정보 노출

조치방법(2)

- 개인정보를 입력하지 않도록 안내

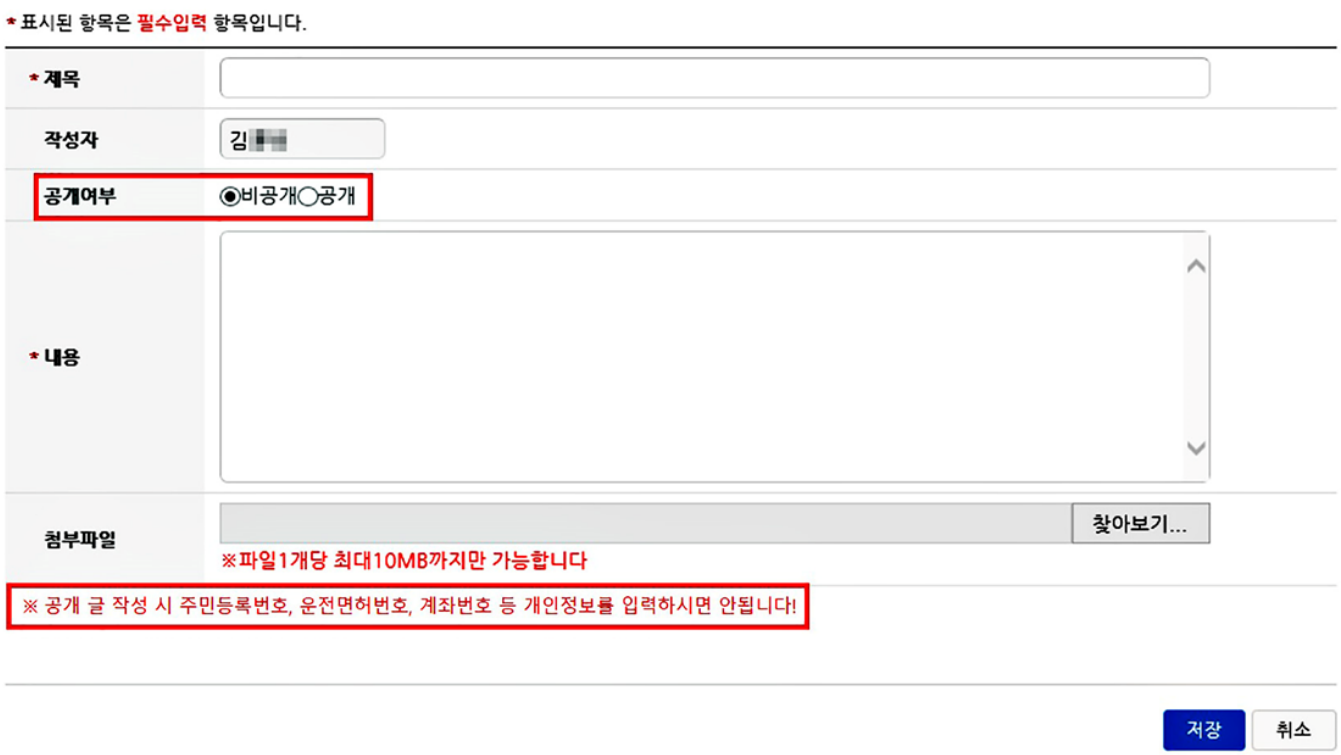


1. 게시글 및 첨부파일에 개인정보 노출

이용자가 문의 글 등을 게시하며 개인정보 노출

조치방법(3)

- 비공개 게시판 운영



개인정보 노출사례 ③

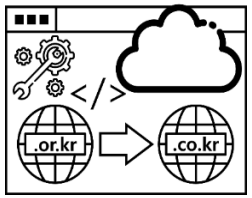
홈페이지 설계·개발 오류

1. 관리자페이지 접근제어 미흡

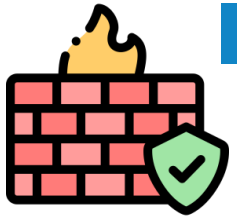
구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

노출사례(1)

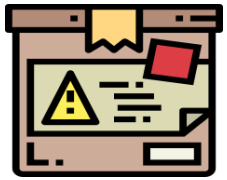
- 구 시스템 방치로 인한 개인정보 노출



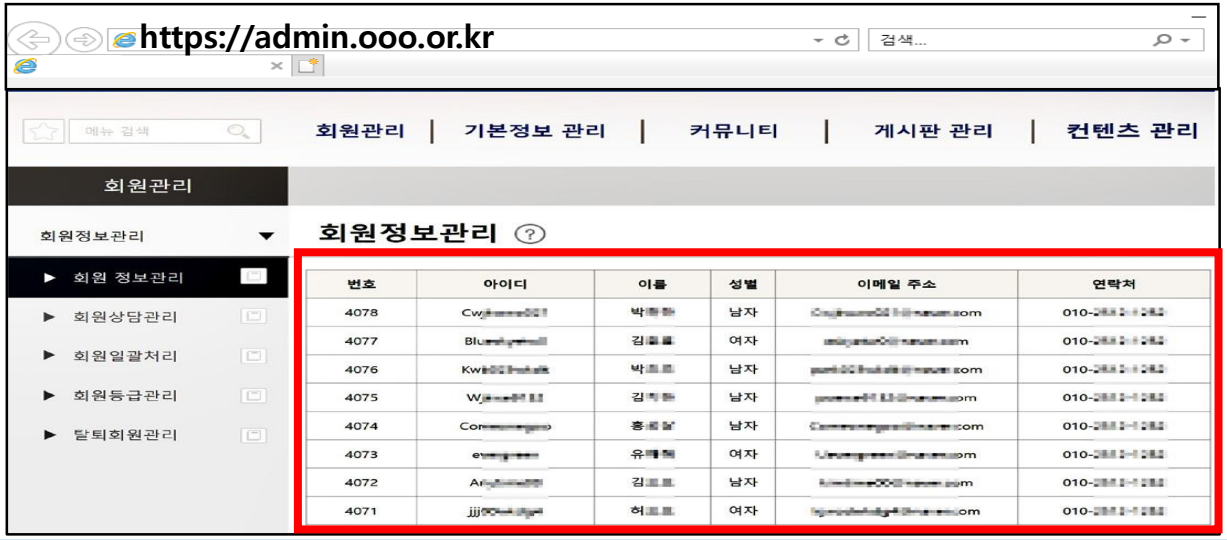
1 새로운 서버로 이전하며 이전 서버를 방치



2 접근통제 미설정 및 파라미터 노출로 비인가자 접근 가능



3 게시판 내에 민원인 파일 노출

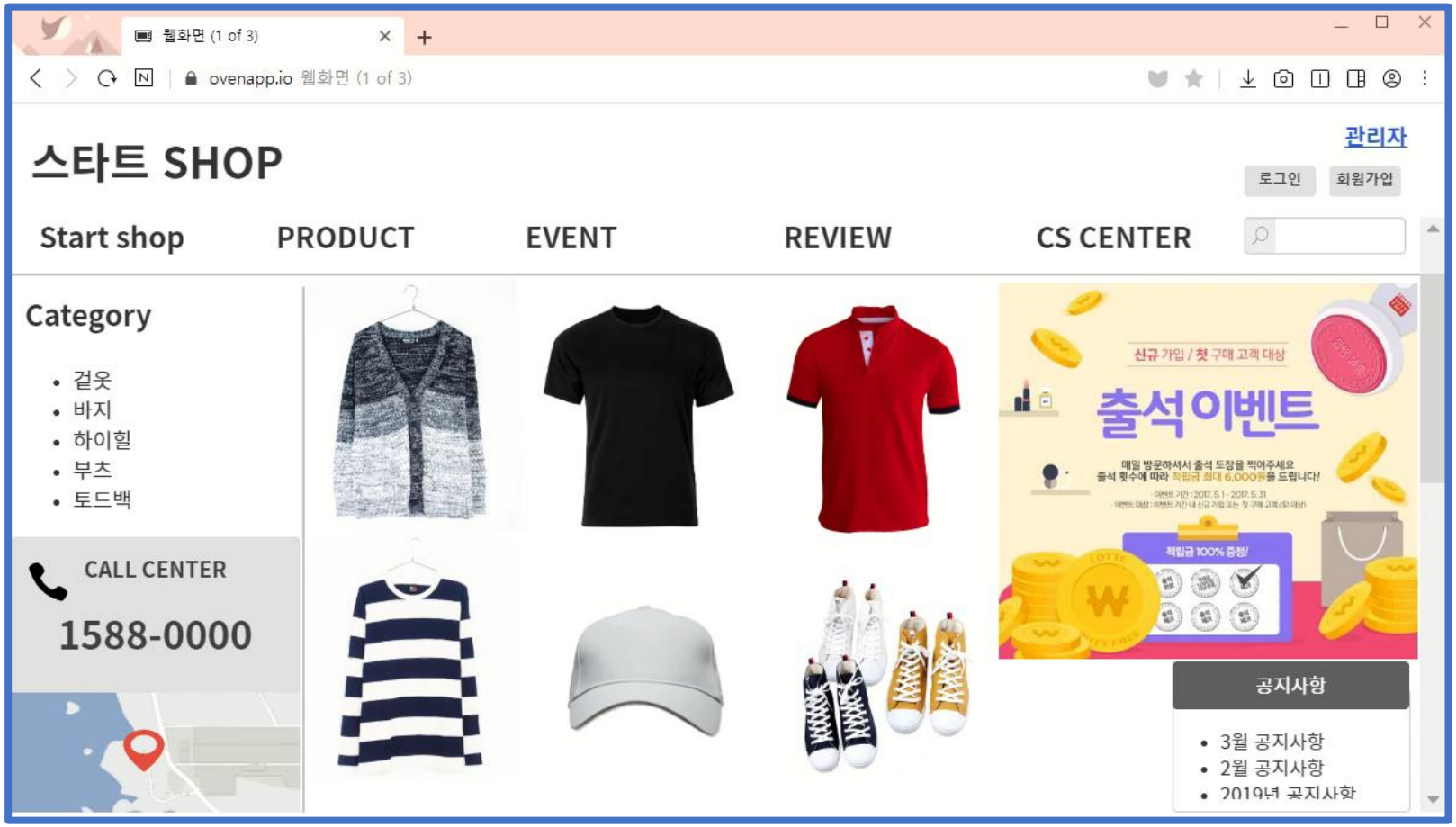


1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

노출사례(2)

- 접근제어 미흡으로 인한 관리자 페이지 노출

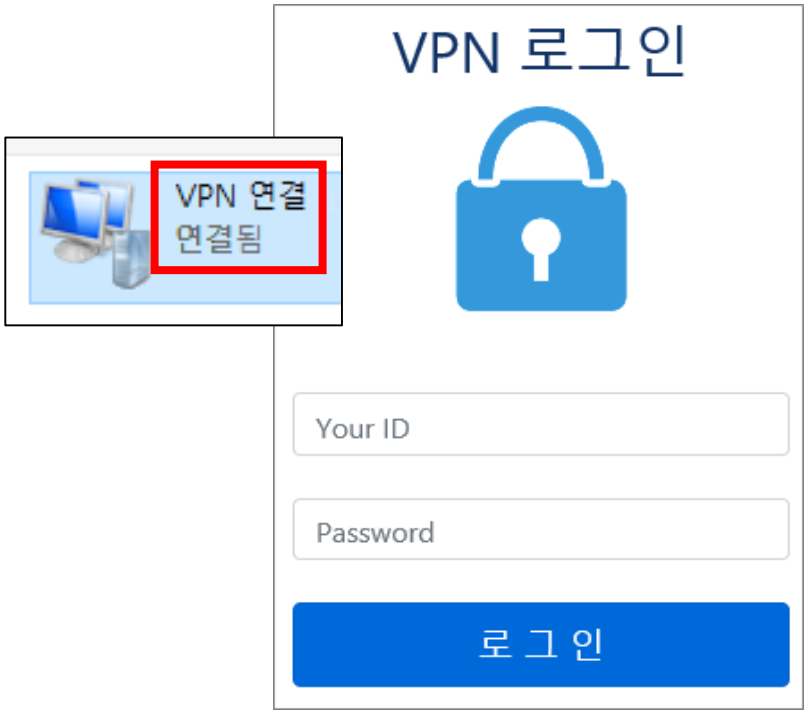


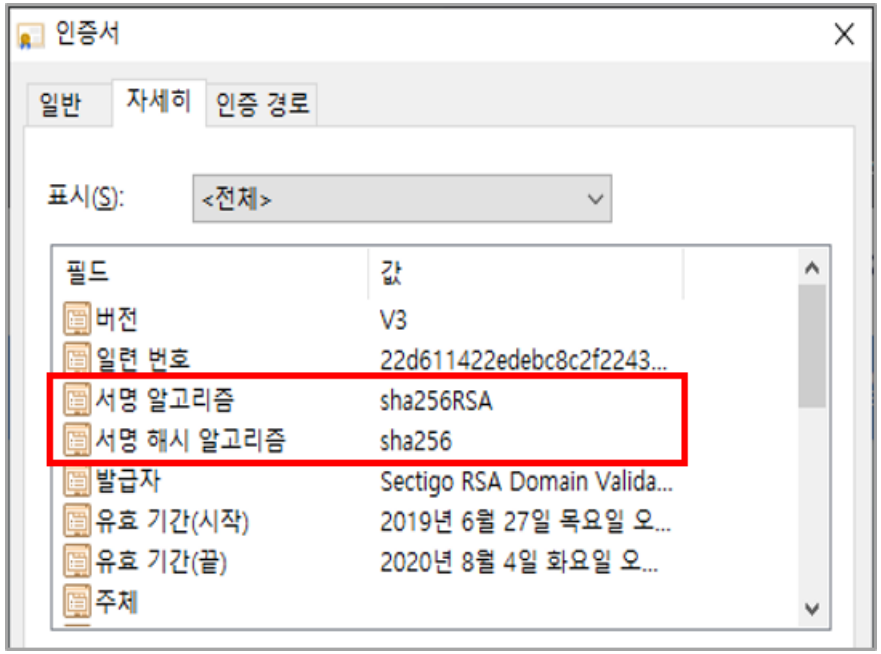
1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(1)

- 안전한 접속수단 마련
  - VPN 접속 또는 SSL 적용



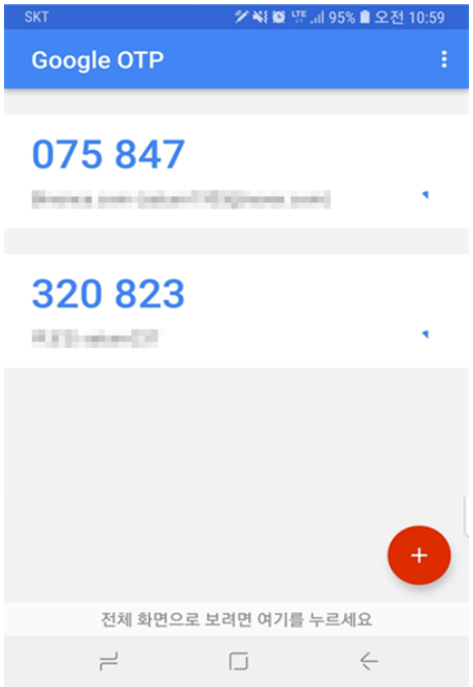


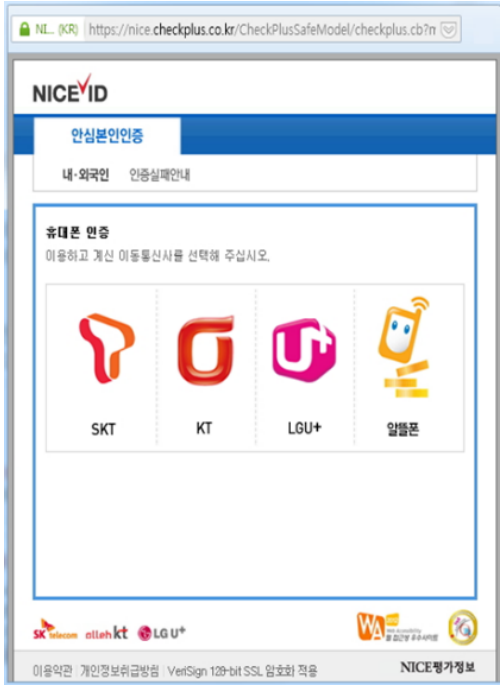
1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(2)

- 안전한 인증수단 마련
  - OTP 인증/ 휴대폰 인증 / 공인인증서 인증



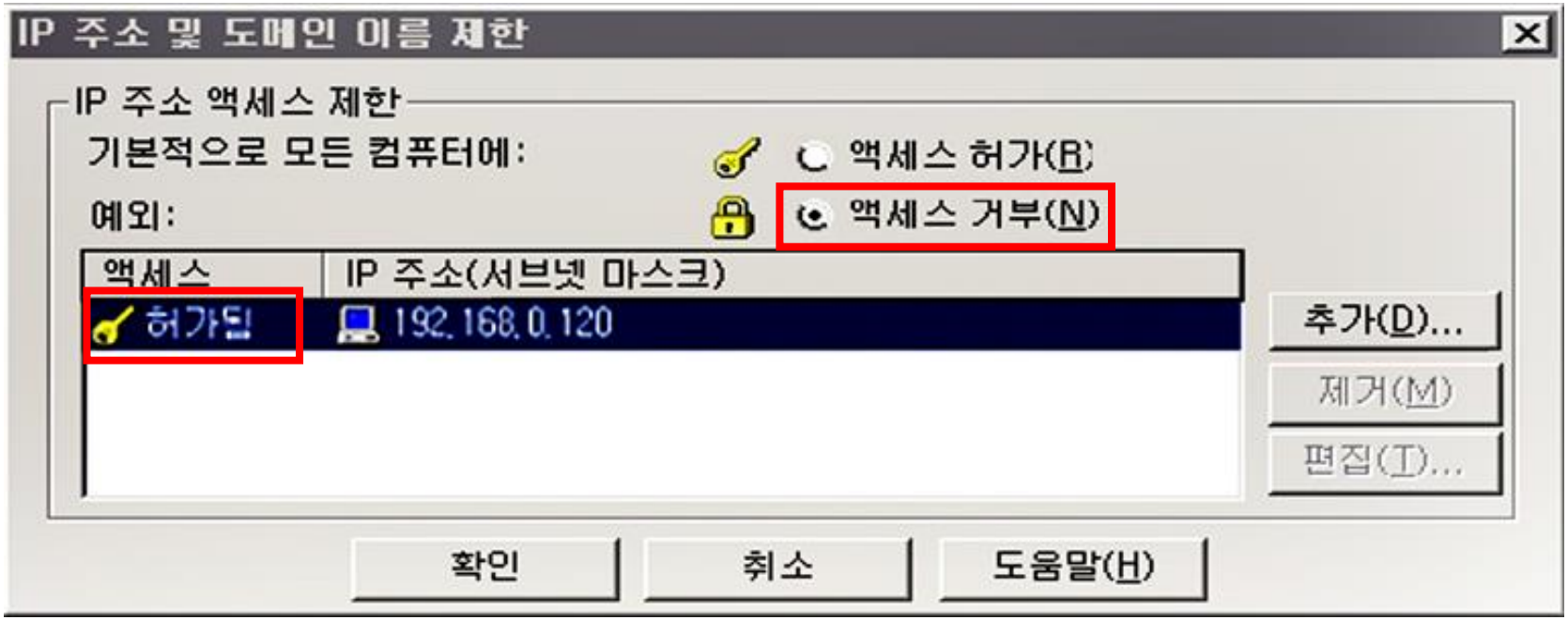


1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(3)

- 특정 IP만 접속 허용하도록 관리자페이지 접근제한

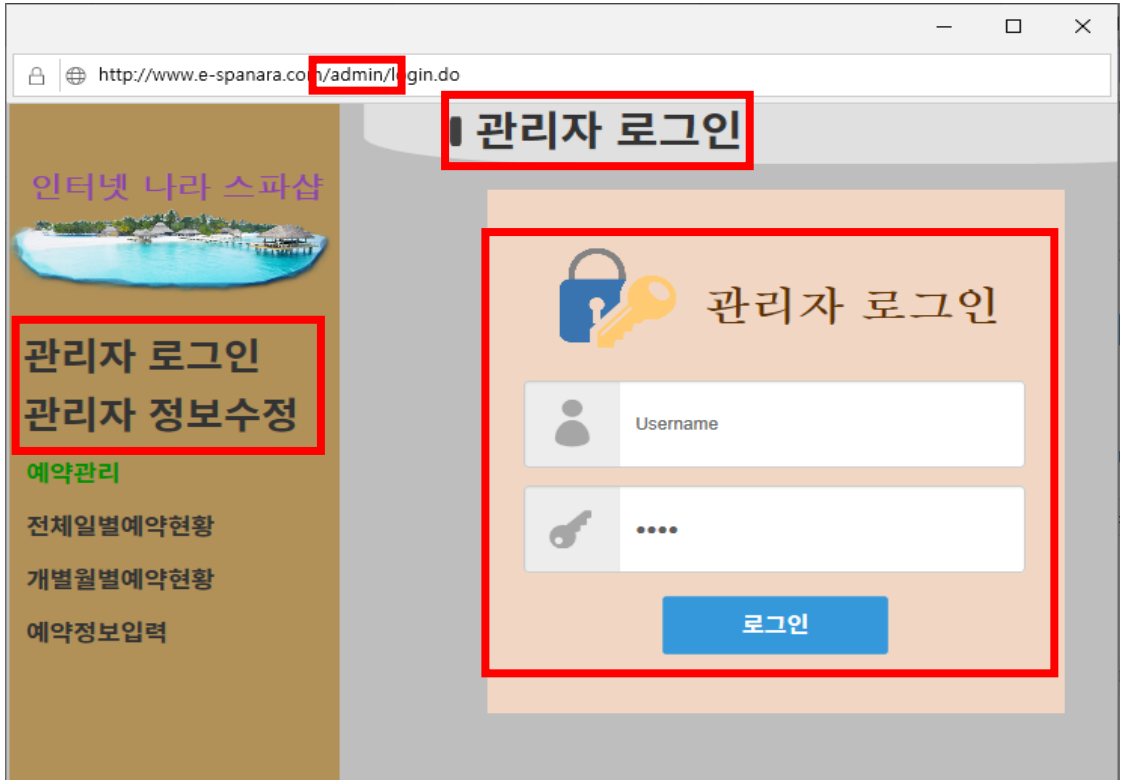


1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(4)

- 일반 이용자가 접근 가능한 관리자 페이지 링크 삭제

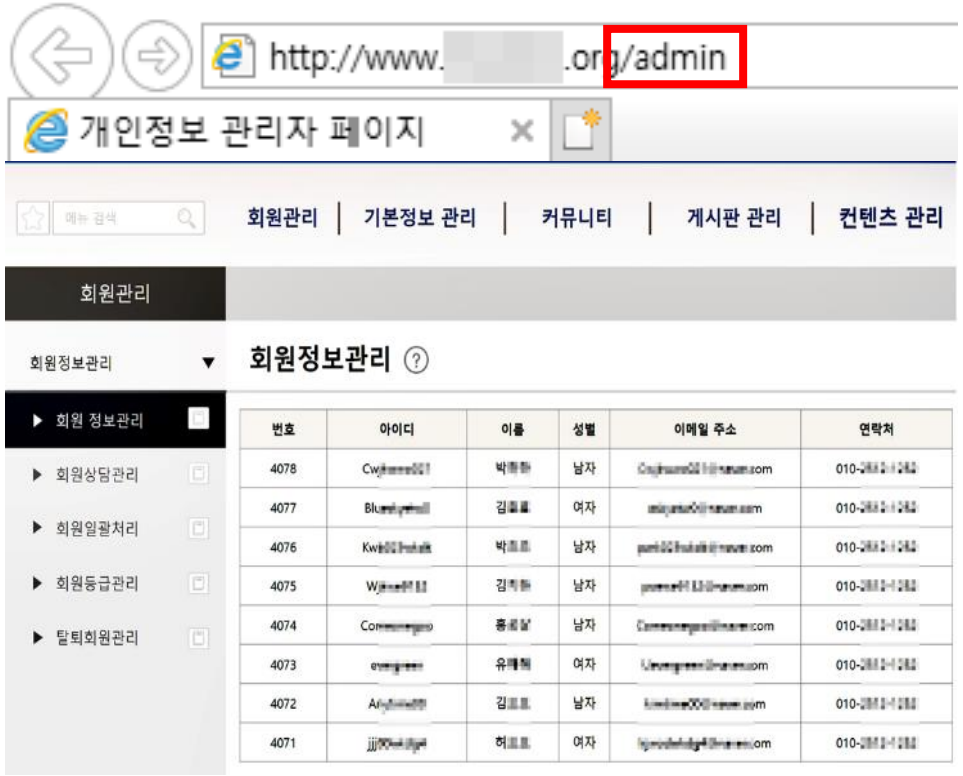


1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(5)

- 쉽게 유추 가능한 관리자 페이지 접속 주소 변경

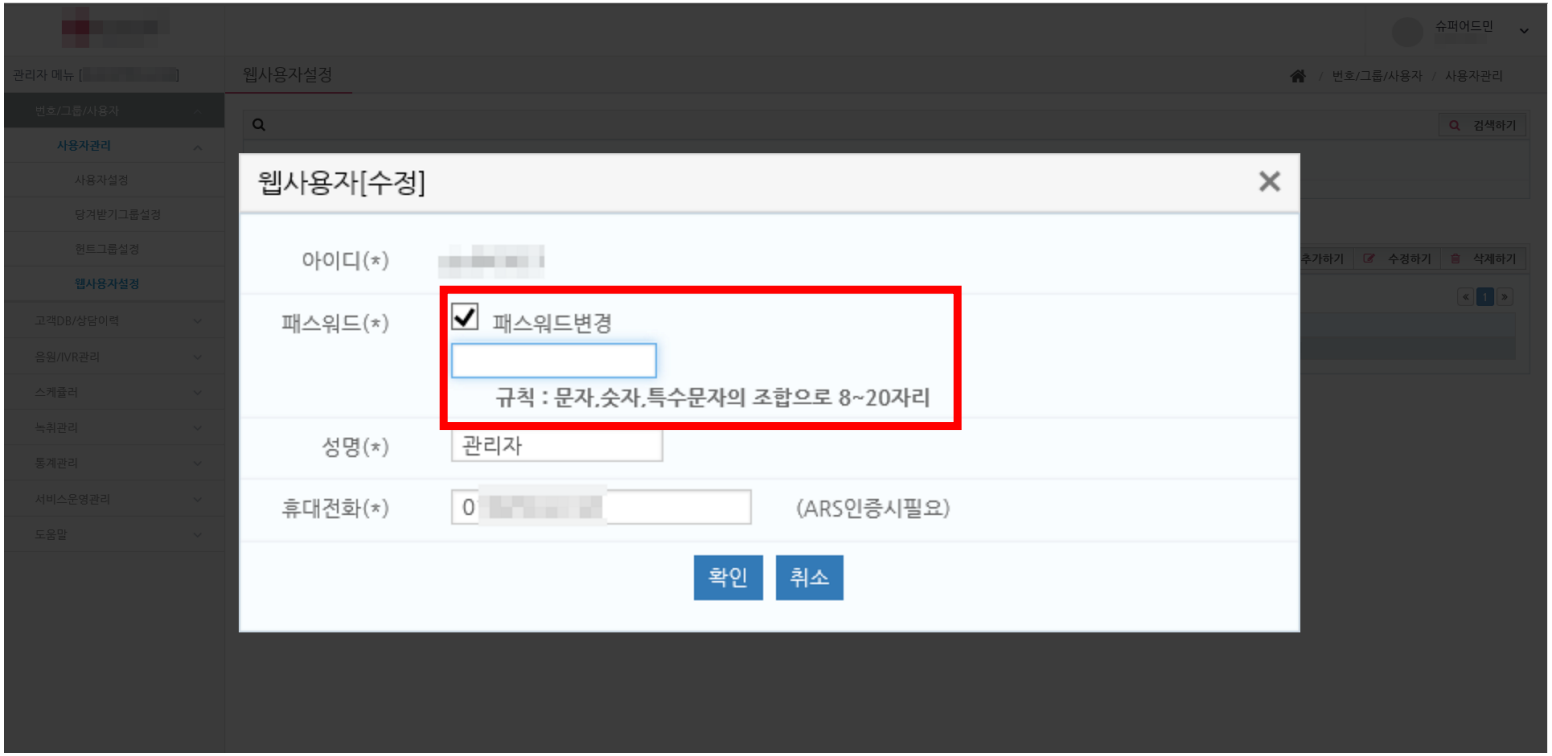


1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(6)

- 주기적인 홈페이지 관리자 비밀번호 변경 및 로그인 시 안전한 비밀번호 사용

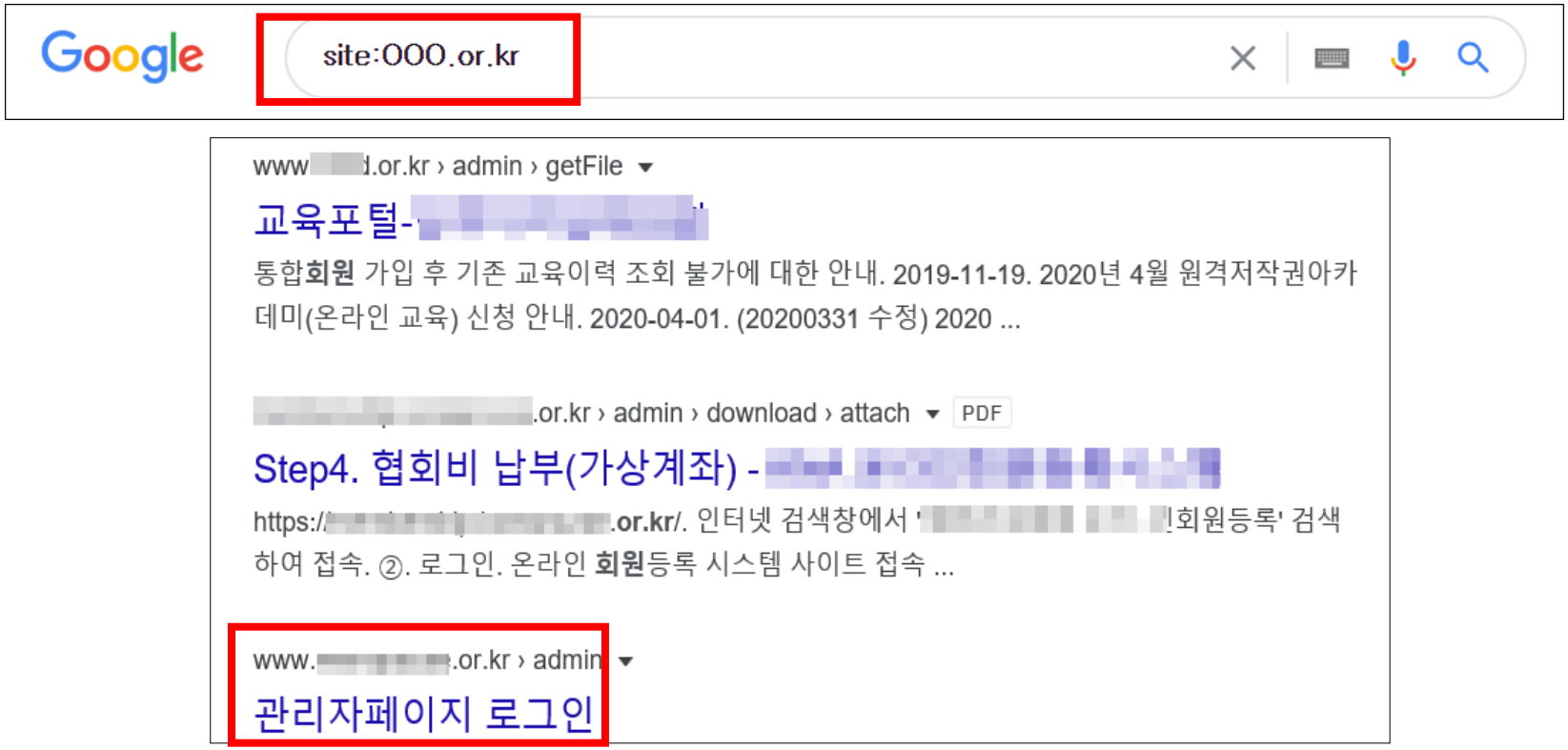


1. 관리자페이지 접근제어 미흡

구 시스템 방치 및 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법(7)

- **검색엔진에 노출여부 확인 및 저장된 페이지 삭제**



2. 홈페이지 접속 경로(URL) 관련 오류

접속 경로(URL)에 개인정보 포함 및 접속 경로(URL) 변경을 통한 개인정보 노출

노출사례(1)

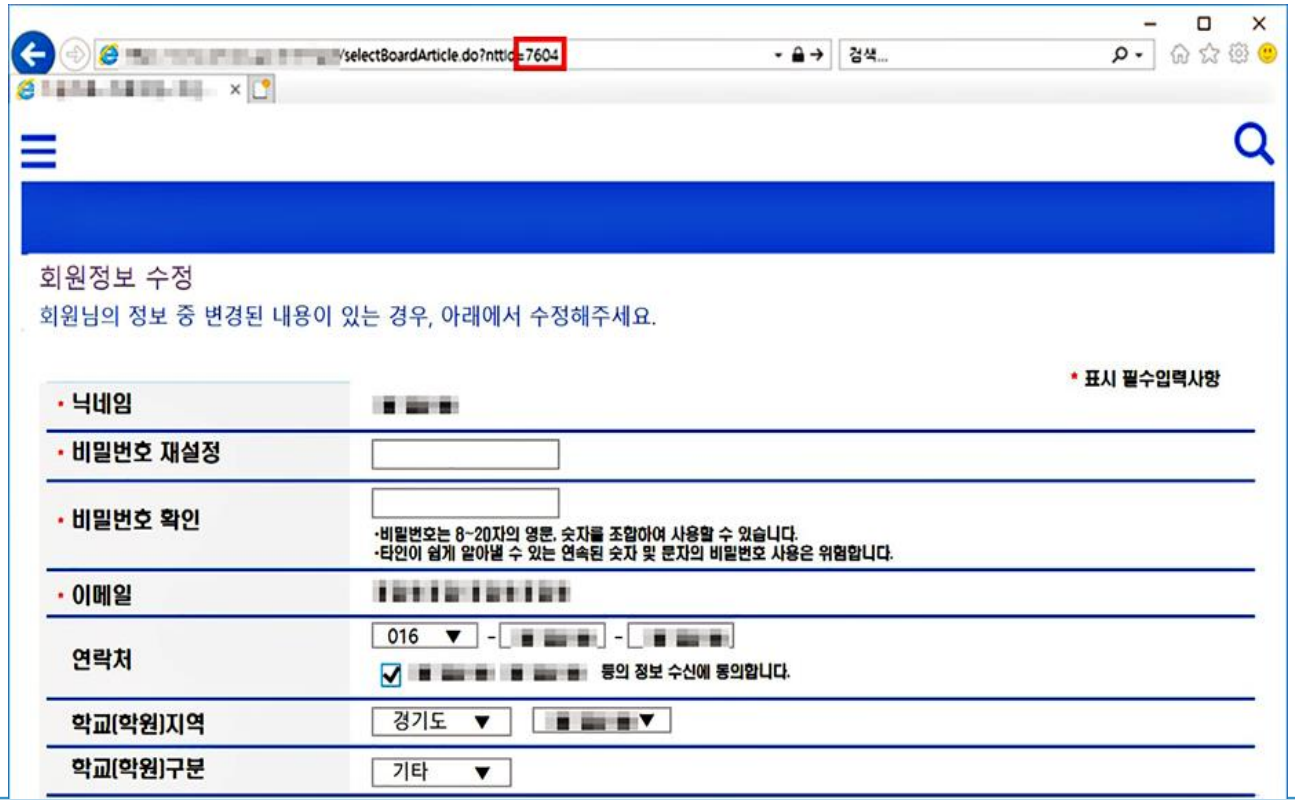
- 접속경로(URL)에 개인정보 포함

2. 홈페이지 접속 경로(URL) 관련 오류

접속 경로(URL)에 개인정보 포함 및 접속 경로(URL) 변경을 통한 개인정보 노출

노출사례(2)

- 접속경로 변경을 통해 타인의 개인정보 열람 및 수정 가능



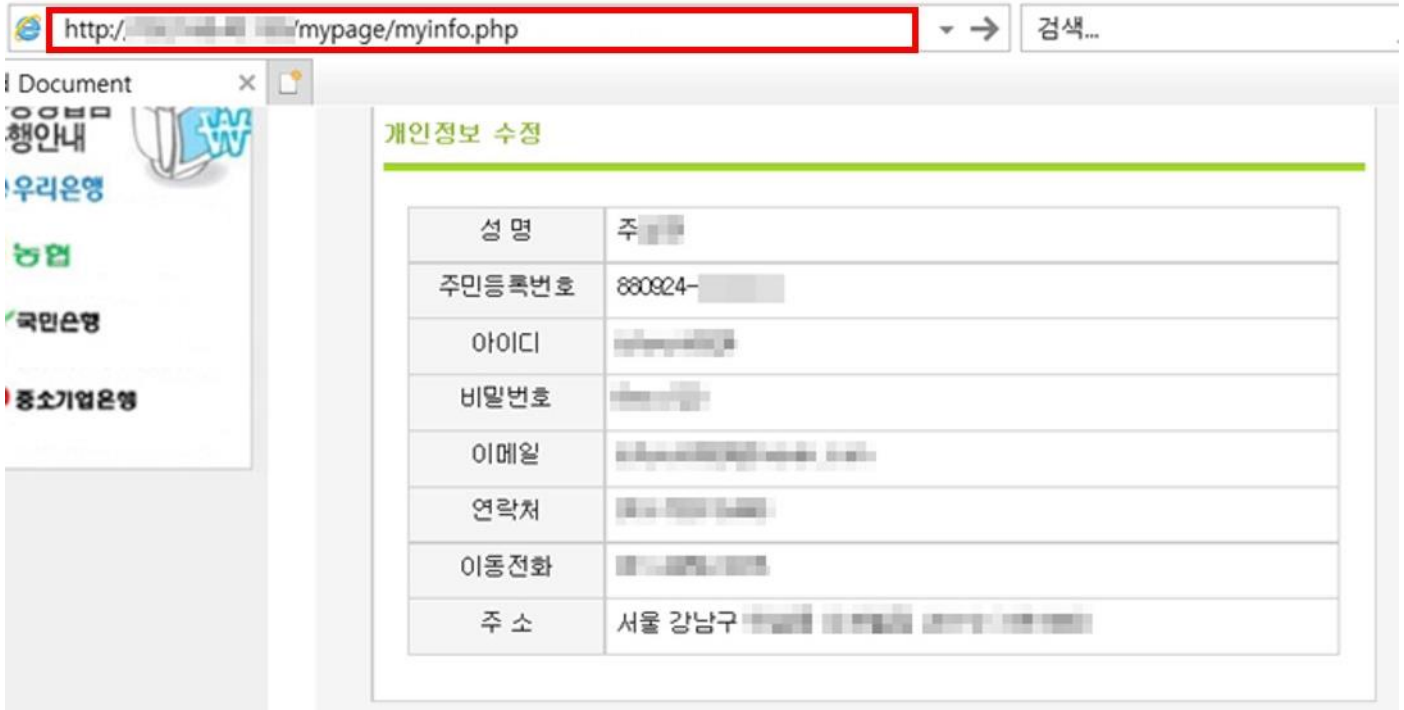
2. 홈페이지 접속 경로(URL) 관련 오류

접속 경로(URL)에 개인정보 포함 및 접속 경로(URL) 변경을 통한 개인정보 노출

조치방법(1)

- 홈페이지 설계 방식 변경
  - 파라미터 방식 변경(GET >POST)

홈페이지 설계 시 POST 방식으로 변경

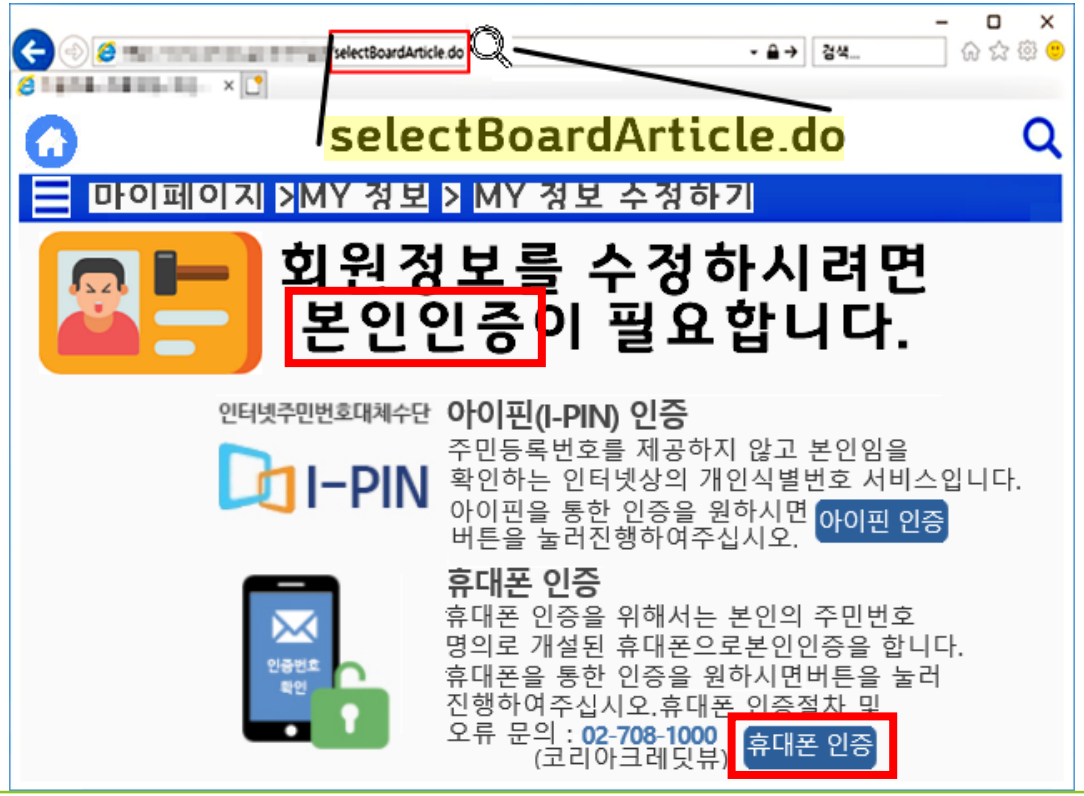


2. 홈페이지 접속 경로(URL) 관련 오류

접속 경로(URL)에 개인정보 포함 및 접속 경로(URL) 변경을 통한 개인정보 노출

조치방법(2)

- 본인 인증 후 회원정보 변경



3. 홈페이지 소스코드 보안설정 미흡

홈페이지 설계 오류로 홈페이지 소스코드에 노출

노출사례

- 소스코드 보기 기능을 통한 개인정보 노출

소스보기

```
  <td width="50%" height="10">작성자 : 주 현</td><a href='?cmd=reply&info_idx=1&member_pno=880924 &b
  <td width="30%" height="10">작성일 : 2018.03.21</td>
</tr>
<tr>
  <td height="25" colspan=3 >제목    : 노트북 특가 이벤트
  </td>
</tr>
<tr align="center">
  <td colspan="3">
    <table width="100%" border="0" cellspacing="2" cellpadding="0" bgcolor="#E3E3E3">
      <tr>
        <td bgcolor="#FFFFFF" align="center"> <br>
          <table width="95%" border="0" cellspacing="0" cellpadding="0">
```

3. 홈페이지 소스코드 보안설정 미흡

홈페이지 설계 오류로 홈페이지 소스코드에 노출

조치방법

- 개인정보 암호화 및 개인 식별용 구분자를 변경, 불필요한 개인정보 삭제

```
<td width="50%" height="10">작성자 : 주 </td>
<td width="30%" height="10">작성일 : 2018.03.21</td>
<a href='?cmd=reply&info_idx=1&member_pno=880924 9b
</tr>
<tr>
  <td height="25" colspan=3 >제목    :
                              노트북 특가 이벤트 </td>
```

주민등록번호

```
<td width="50%" height="10">작성자 : 주 </td>
<td width="30%" height="10">작성일 : 2018.03.21</td>
<a href='?cmd=reply&info_idx=1&member_no=1004 com=yes&gu
</tr>
<tr>
  <td height="25" colspan=3 >제목    :
                              노트북 특가 이벤트 </td>
```

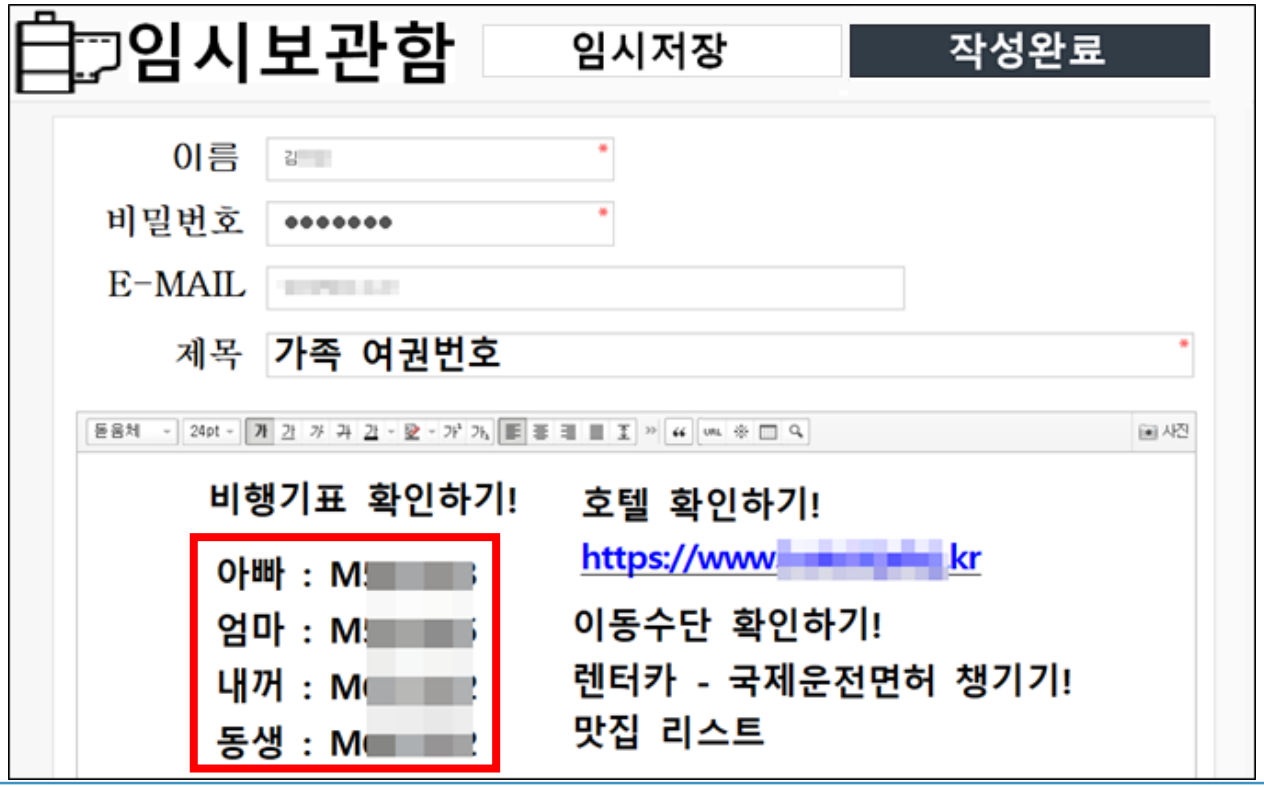
게시글 번호
및 회원 번호

4. 임시저장 페이지 미삭제

이용자 편의를 위한 임시 저장 페이지를 통한 개인정보 노출

노출사례

- 임시보관함에 방치된 개인정보 미삭제로 인한 개인정보 노출

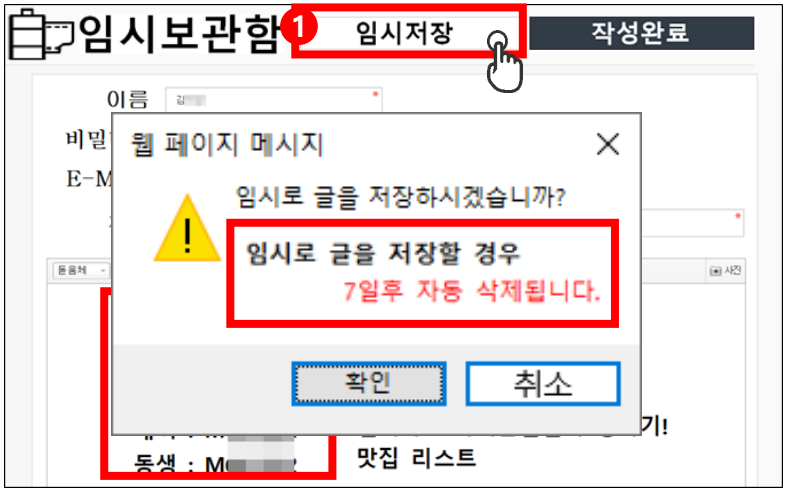


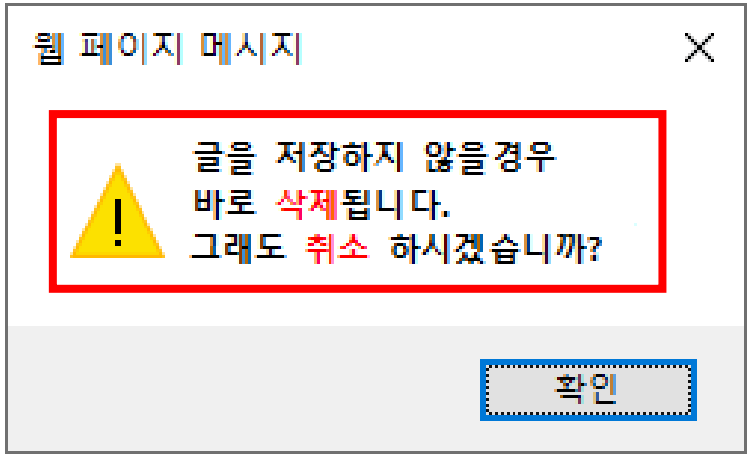
4. 임시저장 페이지 미삭제

이용자 편의를 위한 임시 저장 페이지를 통한 개인정보 노출

조치방법

- 임시저장 페이지 자동 삭제 기능 도입
- 글 작성 취소 시 바로 삭제 조치



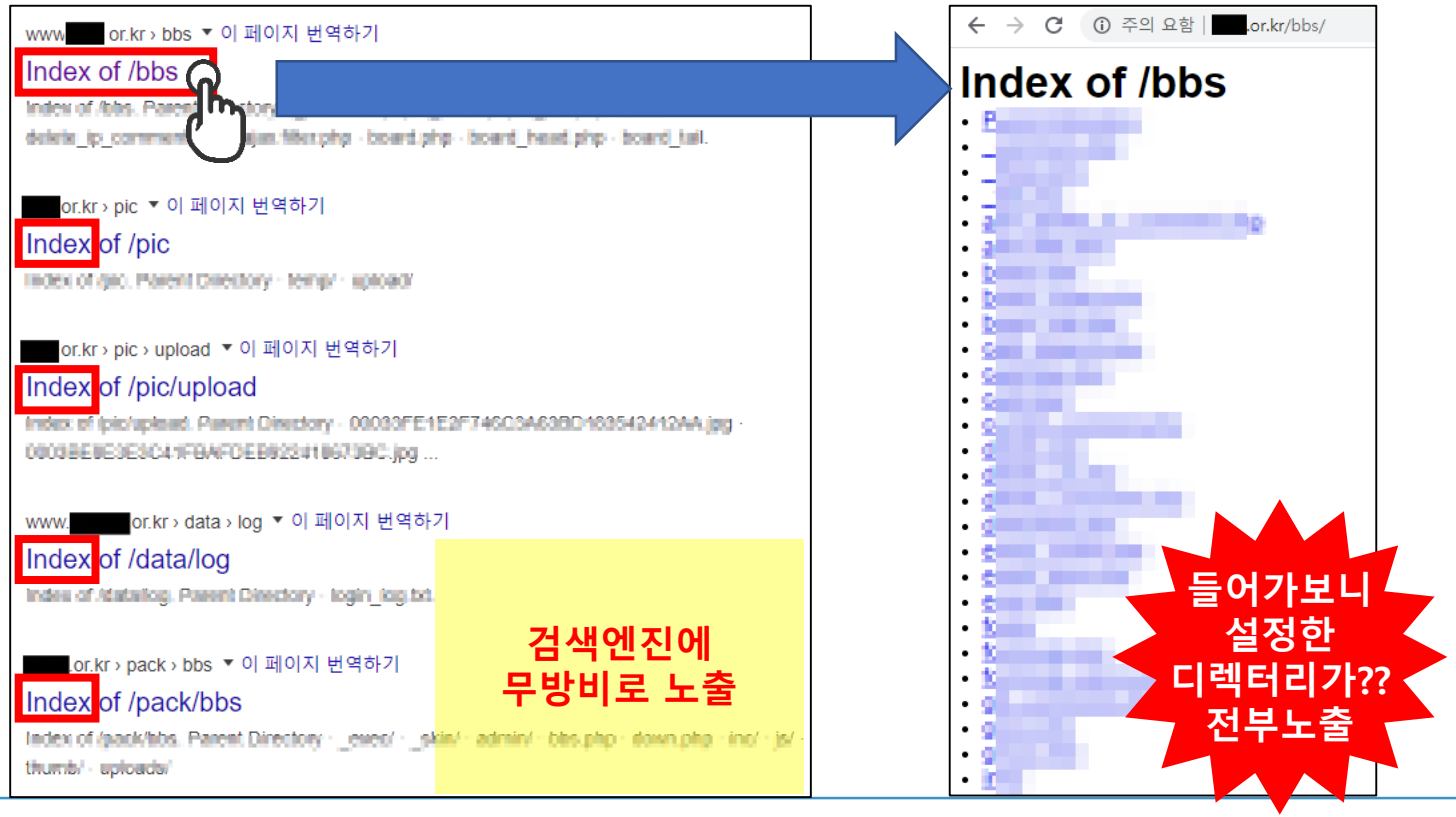


5. 디렉터리 리스팅 보안설정 미흡

디렉터리 리스팅 취약점으로 인해 노출

노출사례

- 웹 서버의 디렉터리 및 파일 노출



5. 디렉터리 리스팅 보안설정 미흡

디렉터리 리스팅 취약점으로 인해 노출

조치방법(1)

- **웹 서버별 디렉터리 리스팅 취약점 해결**

1) Apache 1.x, 2.x : httpd.conf 파일에서 indexes 문자열 제거

```
<Directory "/user/local/server/apache/htdocs">
        Options Indexes 삭제
</Directory>
```

2) Tomcat : web.xml 파일에서 <param-value> 태그 false 로 설정변경

```
<Init-param>
  <param-name>listings</param-name>
  <param-value>false</param-value>
</init-param>
```

3) Nginx : Nginx.conf 파일에서 autoindex 설정을 off 로 변경

```
Location {
    Autoindex off;
}
```

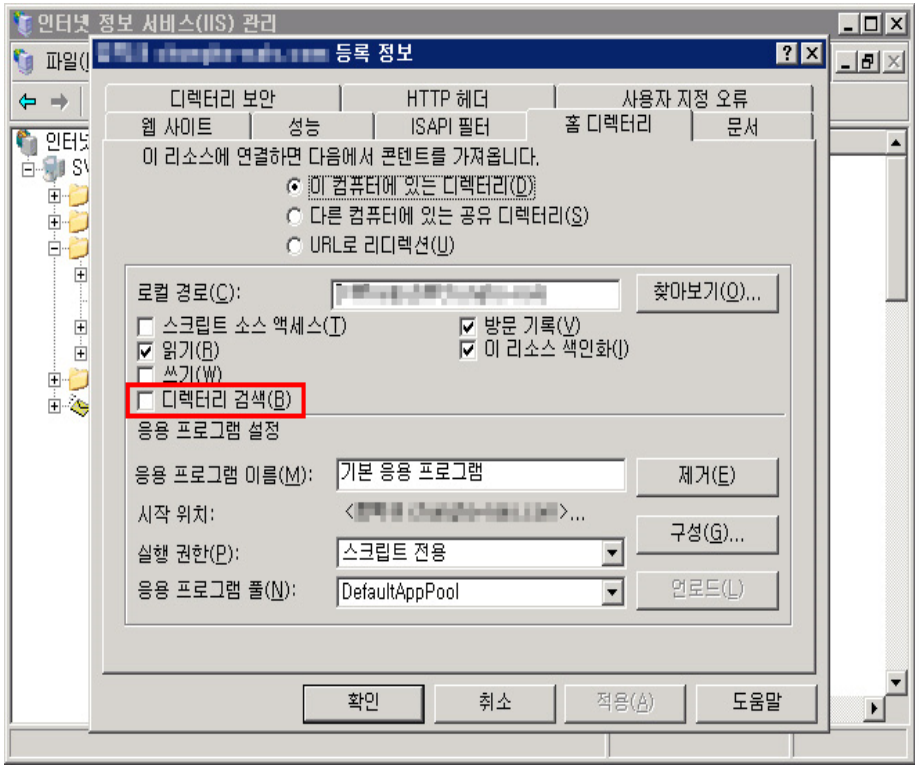
① IIS 6.x 이하
제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 웹사이트의 속성 → 디렉터리 검색 항목 비활성화
② IIS 7.x
제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 웹사이트 홈 → 디렉터리 검색 더블클릭 → 우측 작업창에서 사용 해제
③ IIS 8.x
제어판 → 시스템 및 보안 → 관리도구 → IIS(인터넷 정보서비스) 관리자 → 사이트 → 기본 웹사이트 홈 →
디렉터리 검색을 더블클릭 → 우측 작업창에서 사용 해제

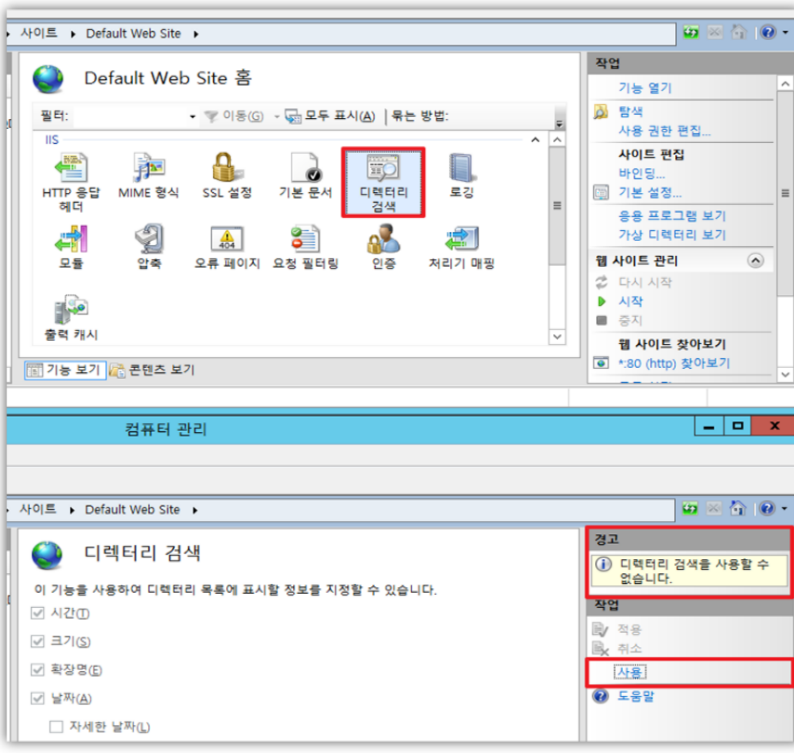
5. 디렉터리 리스팅 보안설정 미흡

디렉터리 리스팅 취약점으로 인해 노출

조치방법(2)

- 웹 서버별 디렉터리 리스팅 취약점 해결





KISA 한국인터넷진흥원

Ⅲ. 개인정보 노출 점검 실습

1. 개인정보 노출 자가 점검
2. 검색 기능
3. 검색엔진 페이지 삭제 방법

1. 개인정보 노출 자가 점검

검색엔진을 통한 개인정보 노출 점검

- 기관은 검색엔진을 통해 개인정보가 노출되고 있는지 모니터링 가능
- 자사 사이트의 개인정보 노출 여부를 주기적으로 점검하고, 노출 되었다면 즉시 조치 필요

< 주요 노출 키워드(예시) >

번호	탐지어	번호	탐지어
1	주민등록번호	7	여행 문의 + 여권번호
2	여권번호	8	회원명단 filetype:xls
3	운전면허번호	9	입사지원서 filetype:xls
4	외국인등록번호	10	주민등록번호 txt
5	이력서 filetype:doc	11	학생명단 xlsx
6	이력서 filetype:xls	12	교육생 명단 filetype:xls

2. 검색 기능

검색엔진이 수집한 내용 찾기

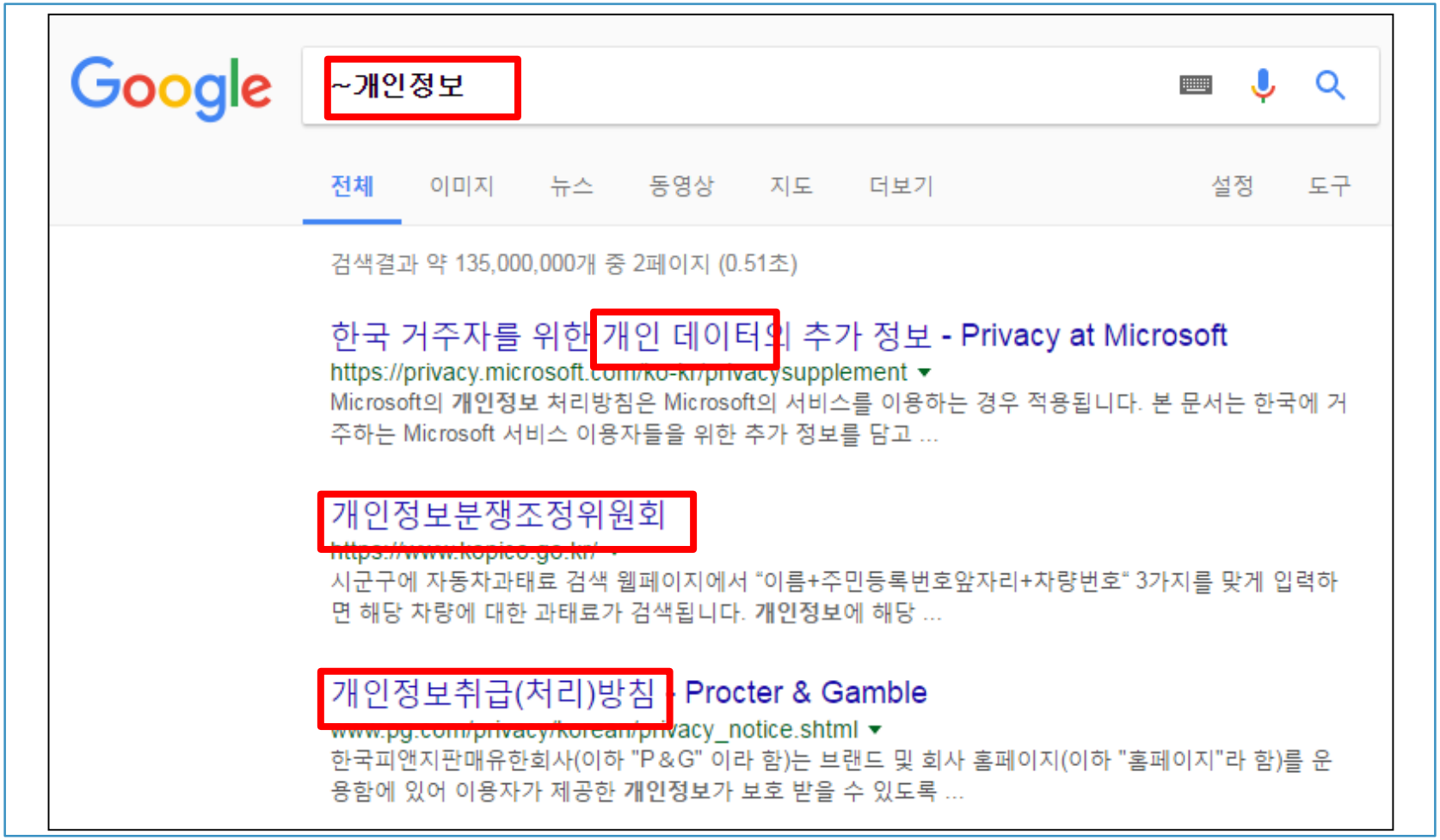
연산자	설명	형식
“”	정확한 문구를 포함한 결과를 검색	“검색어”
~	검색어와 비슷한 결과를 검색	~검색어
and, 공백	둘 다 포함한 결과 검색	검색어A and 검색어B
OR(대문자), |	둘 중에 하나 포함 결과 검색	검색어A | 검색어B
- (마이너스)	원하지 않는 단어를 제외하고 검색	-검색어
define	특정 단어의 정의를 검색	define:검색어
site	검색 범위를 특정 도메인으로 제한 검색	site:kisa.or.kr 검색어
intitle	페이지의 제목에서 문자열을 검색	intitle:검색어
inurl	문자열을 페이지의 URL에서 검색	inurl:검색어
filetype	특정한 확장자를 가진 파일을 검색	filetype:‘파일형식‘
#..#	..앞뒤로 지정된 숫자 범위 안에 있는 결과값을 나타냄	검색어 #..#

2. 검색 기능 > 정확한 문구 검색

- 검색어의 처음과 끝에 큰 따옴표(“)를 입력하면
  해당 단어나 문장이 반드시 포함된 사이트를 검색할 수 있음

2. 검색 기능 > 비슷한 의미의 검색

- 검색어 앞에 '물결표시(~)'를 입력하면 검색어와 비슷한 의미를 가진 자료를 보여줌



2. 검색 기능 > 두 가지 문구 모두 포함하여 검색

- 검색어 사이에 'and' 또는 공백을 포함하면 검색어 둘 다 포함한 결과가 검색됨

2. 검색 기능 > 두 가지 문구 중 하나라도 포함하여 검색

- 검색엔진에서 검색어 사이에 'OR' 또는 '|' 포함하면 둘 중 하나가 포함되도록 검색됨

2. 검색 기능 > 원하지 않는 단어를 제외하고 검색

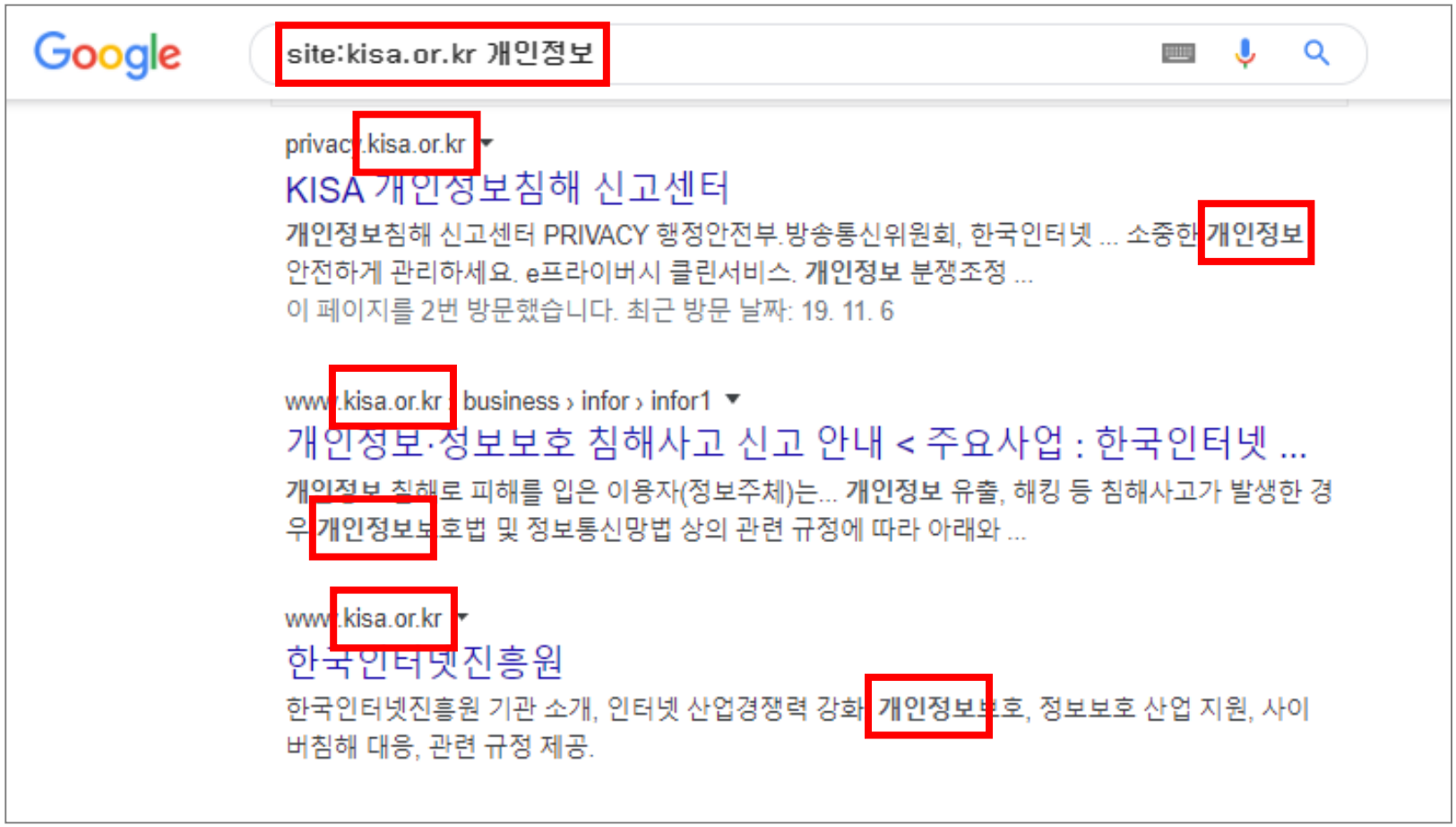
- 검색 시 '-OOO'를 포함하면 검색어에서 원치 않는 단어가 제외되고 검색됨

2. 검색 기능 > 단어의 정의 검색

- 검색어 창에 ‘define:특정단어’ 입력하면 해당 검색어의 정의를 보여줌

2. 검색 기능 > 특정 도메인 내 검색

- 검색어 앞에 'site:사이트'를 포함하면 해당 사이트에서 검색됨

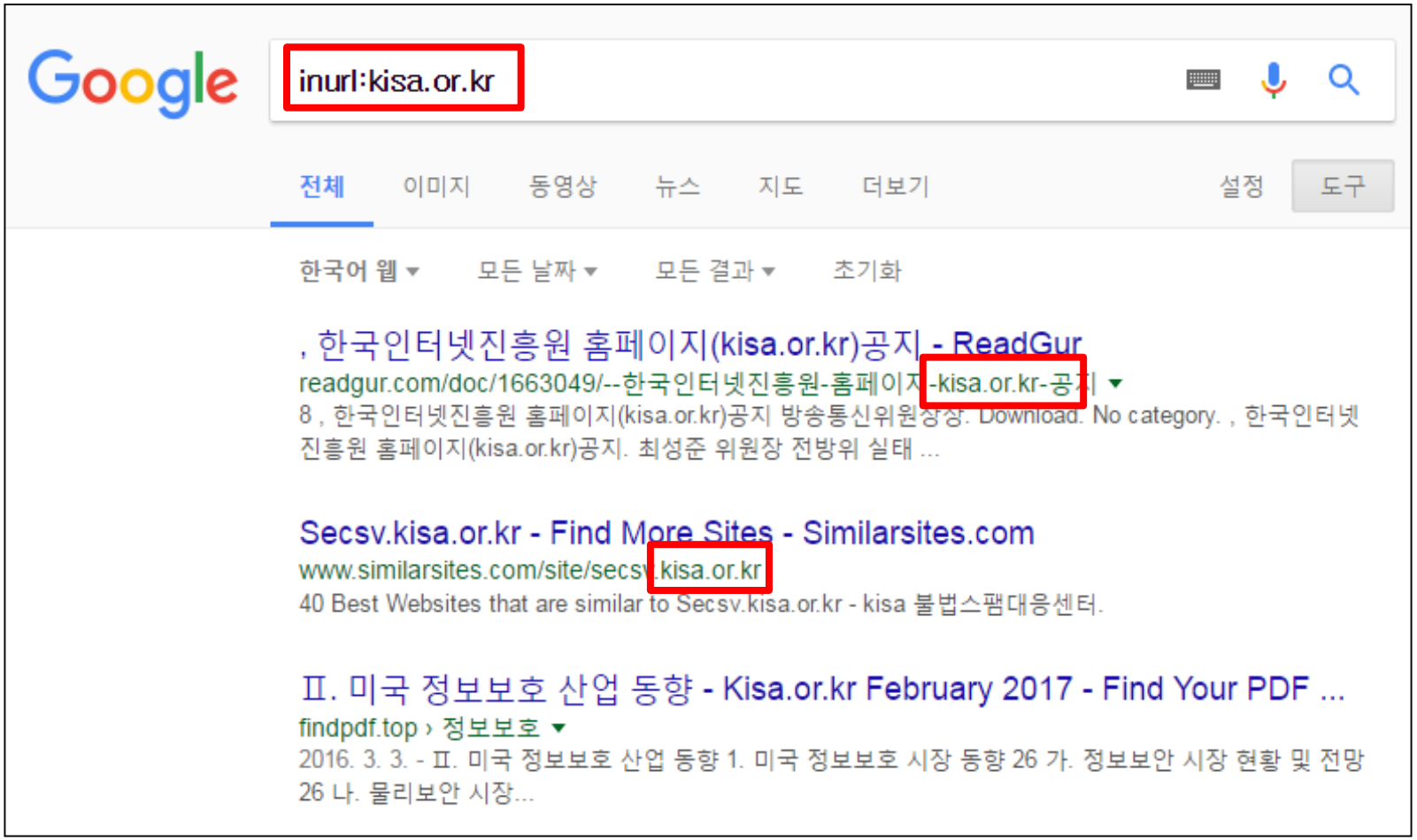


2. 검색 기능 > 제목 특정단어 포함 검색

- 검색어 창에 ‘intile:특정단어’를 입력하면 제목에 특정단어가 포함된 결과가 검색됨

2. 검색 기능 > 특정 사이트 문서 검색

- 검색어 창에 'Inurl:특정사이트'를 검색하면 검색어에 해당하는 사이트가 검색됨



2. 검색 기능 > 특정 파일 type 문서 검색

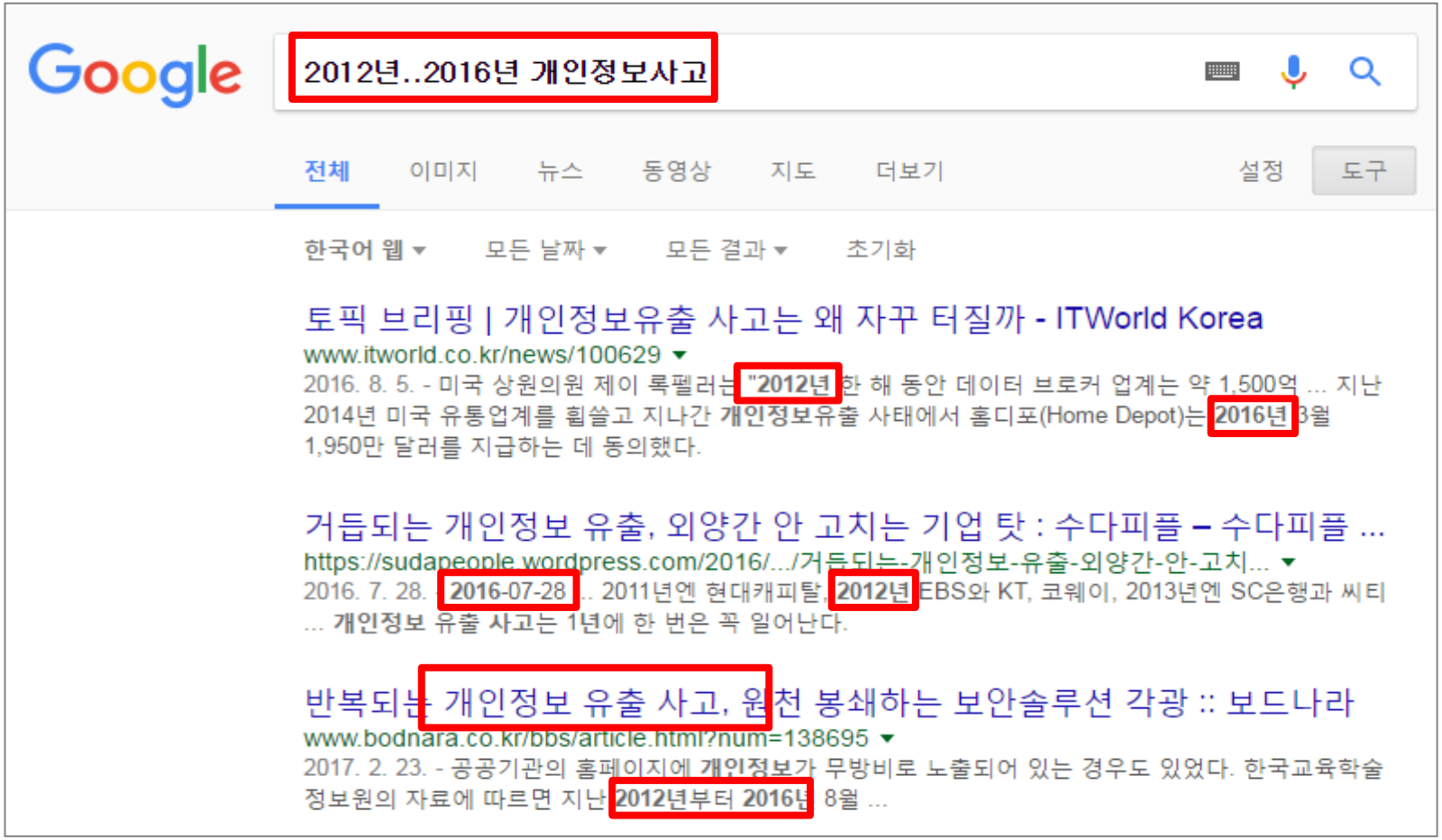
- 검색어 앞에 'filetype:OOO'를 포함하면 검색어에 해당하는 file이 검색됨

※ 파일타입

① .doc
② .xls
③ .hwp
④ .pdf 등

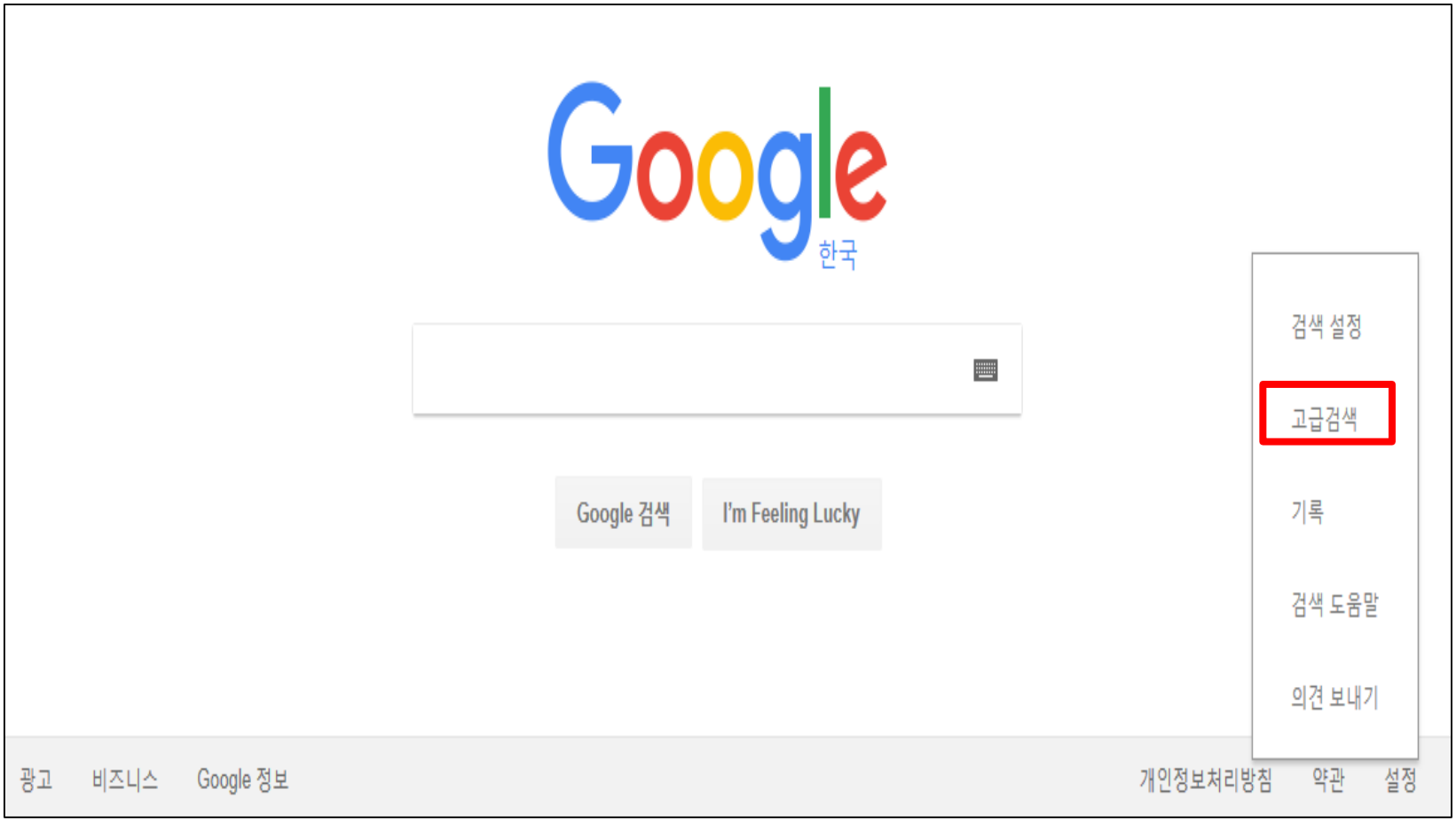
2. 검색 기능 > 특정 범위의 결과 검색

- 검색할 숫자 사이에 마침표 2개(..)를 입력하여 검색하면 숫자 범위 내, 검색결과를 보여줌



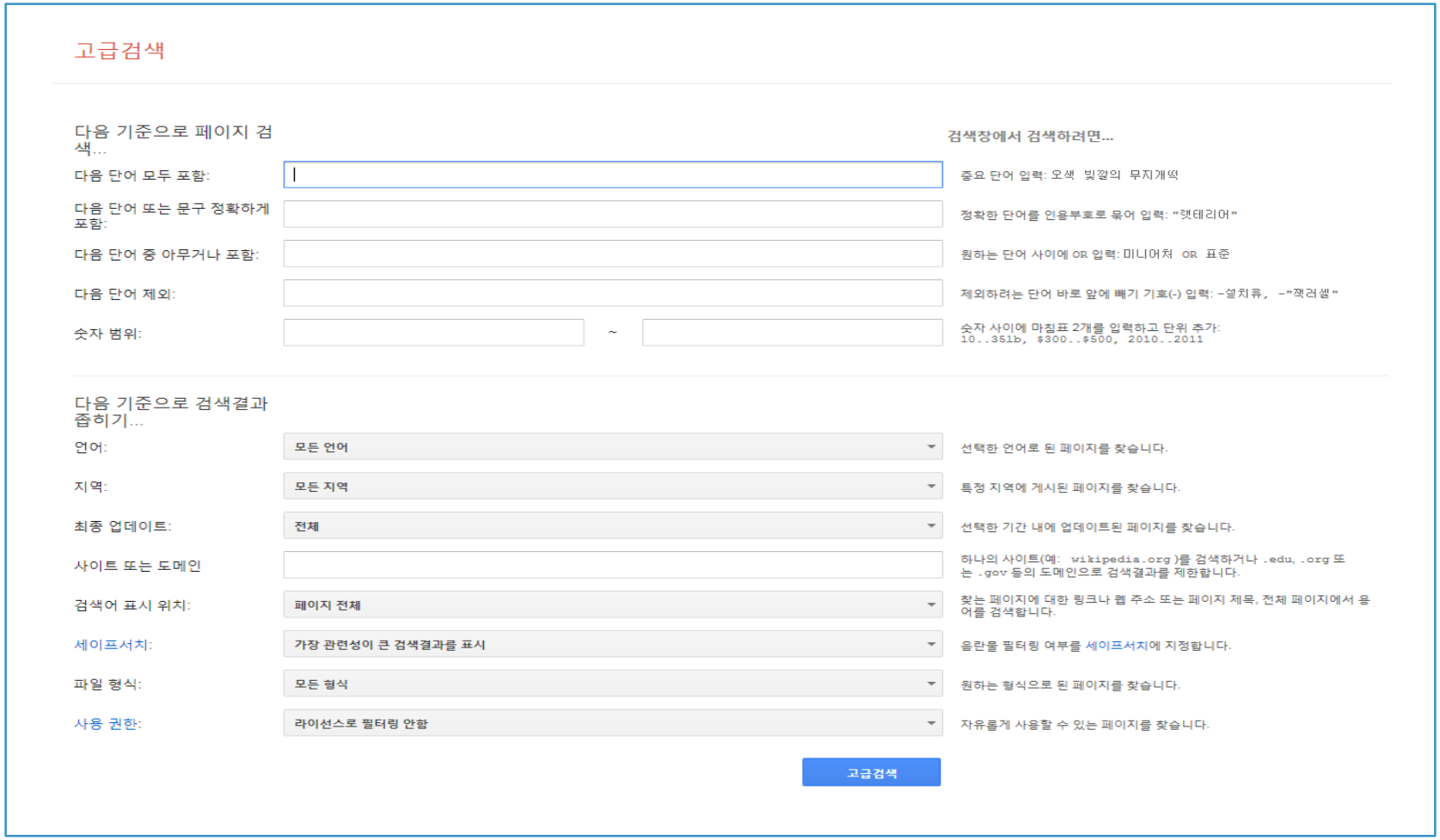
2. 검색 기능 (설정 > 고급검색)

설정 메뉴를 통한 고급검색 방법



2. 검색 기능 (설정 > 고급검색)

설정 메뉴를 통한 고급검색 방법



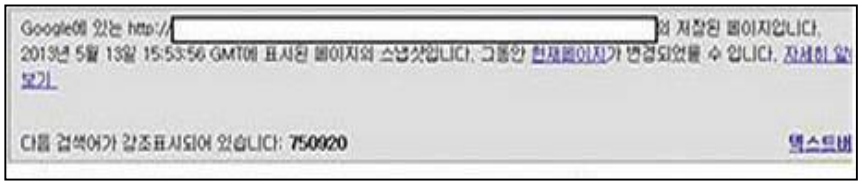
3. 검색엔진에 저장된 페이지 삭제

검색엔진(구글, 네이버, 다음 등)에 노출된 값을 입력하여 검색결과값 확인

조치방법

Step 1. 홈페이지에 노출된 개인정보 페이지를 삭제
Step 2. 검색엔진에 홈페이지의 노출 개인정보 URL 또는 노출된 값을 입력하여 검색결과 값 확인
Step 3. 검색결과 캐시페이지에 개인정보가 존재할 경우 해당 페이지 삭제 요청

검색엔진에 노출 확인

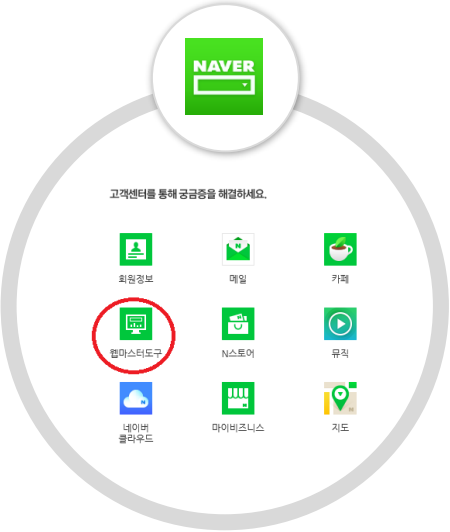


3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 캐시페이지 삭제 요청 주소

https://www.google.com/webmasters/tools/removals

오래된 콘텐츠 삭제



https://help.naver.com/support/home.nhn

웹마스터도구

https://cs.daum.net/redbell/top.html

권리침해신고

고객센터(CS)

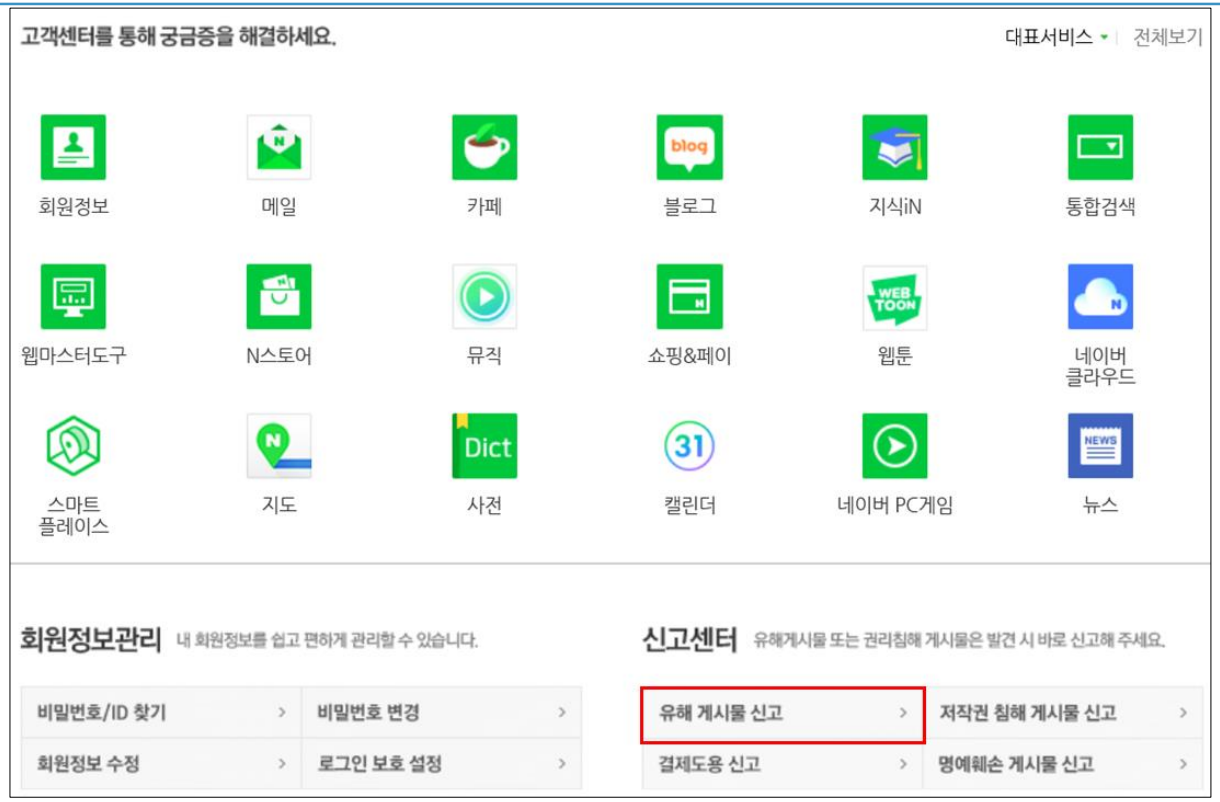
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 네이버 저장된 페이지 삭제 방법

① 네이버 고객센터 방문

네이버 고객센터 > 신고센터 > 유해 게시물 신고



3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

▪ 네이버 저장된 페이지 삭제 방법

② 네이버 게시물 신고 접수

게시물 신고접수 > 신고하는 이유(개인정보 노출) 선택

3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

▪ 네이버 저장된 페이지 삭제 방법

③ 노출되는 위치 선택

개인정보 노출이 발생한 게시물이 어디에서 노출되고 있는지 선택(네이버 검색결과)

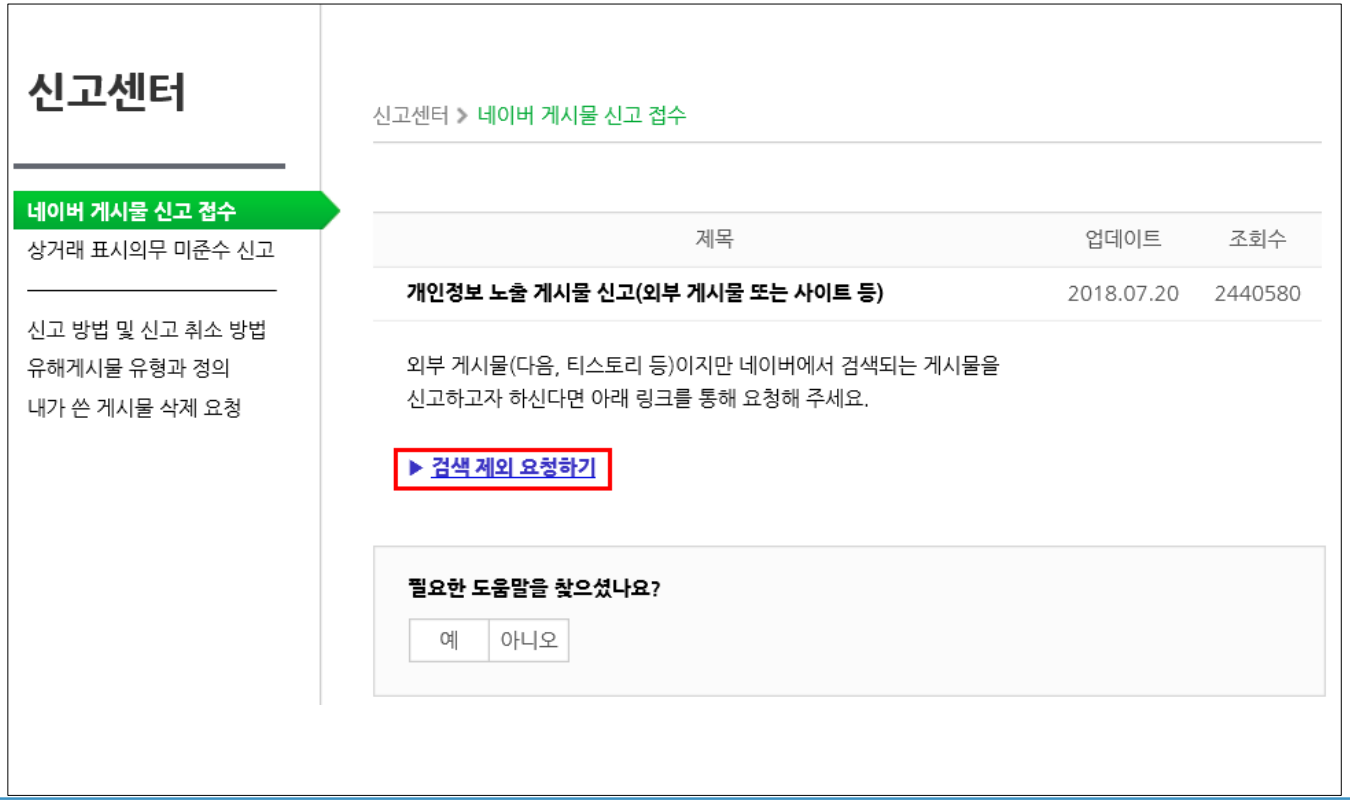
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

▪ 네이버 저장된 페이지 삭제 방법

④ 검색 제외 요청하기

검색엔진에서 노출되는 게시물을 검색 제외하기 위해 '검색 제외 요청하기' 메뉴 선택



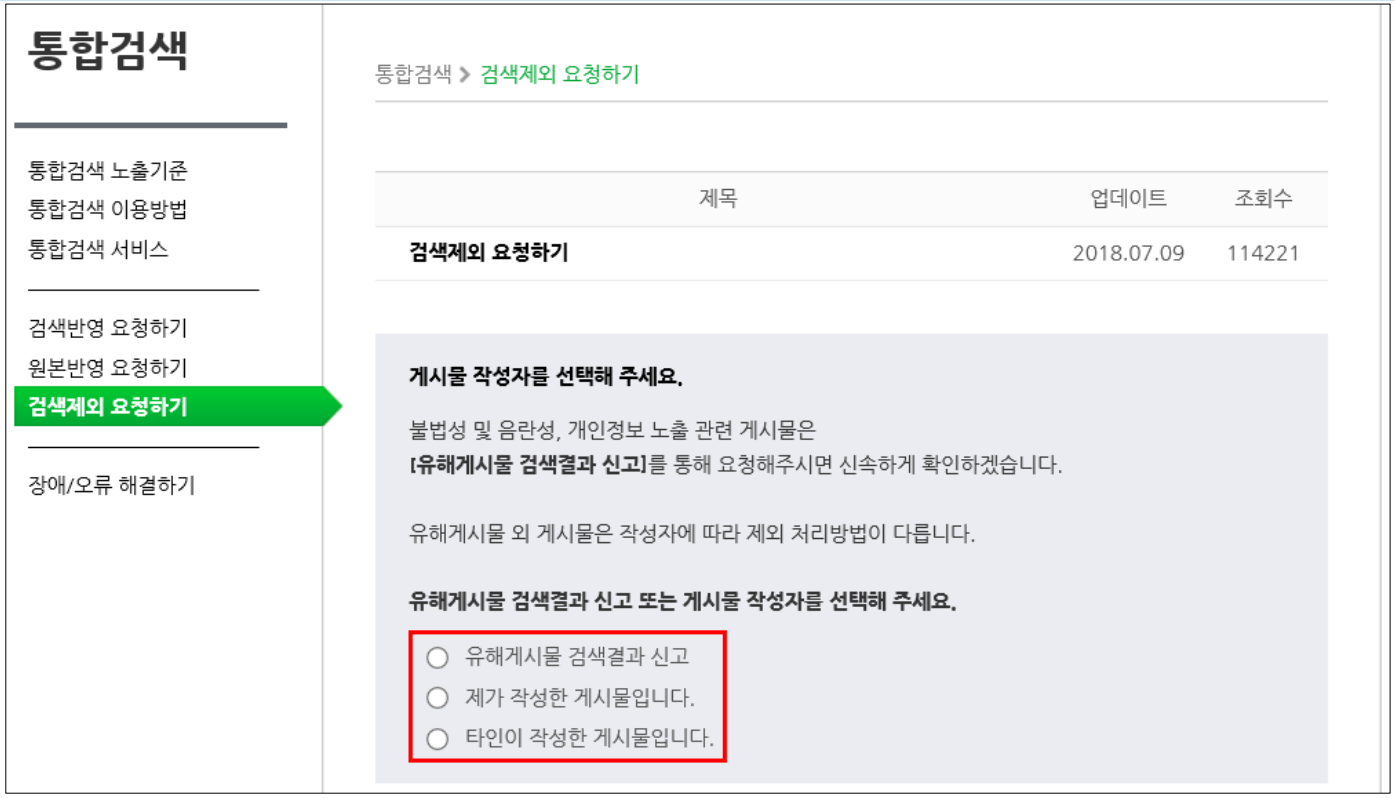
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 네이버 저장된 페이지 삭제 방법

⑤ 게시물의 작성자 선택

개인정보가 노출된 게시물의 작성자 선택



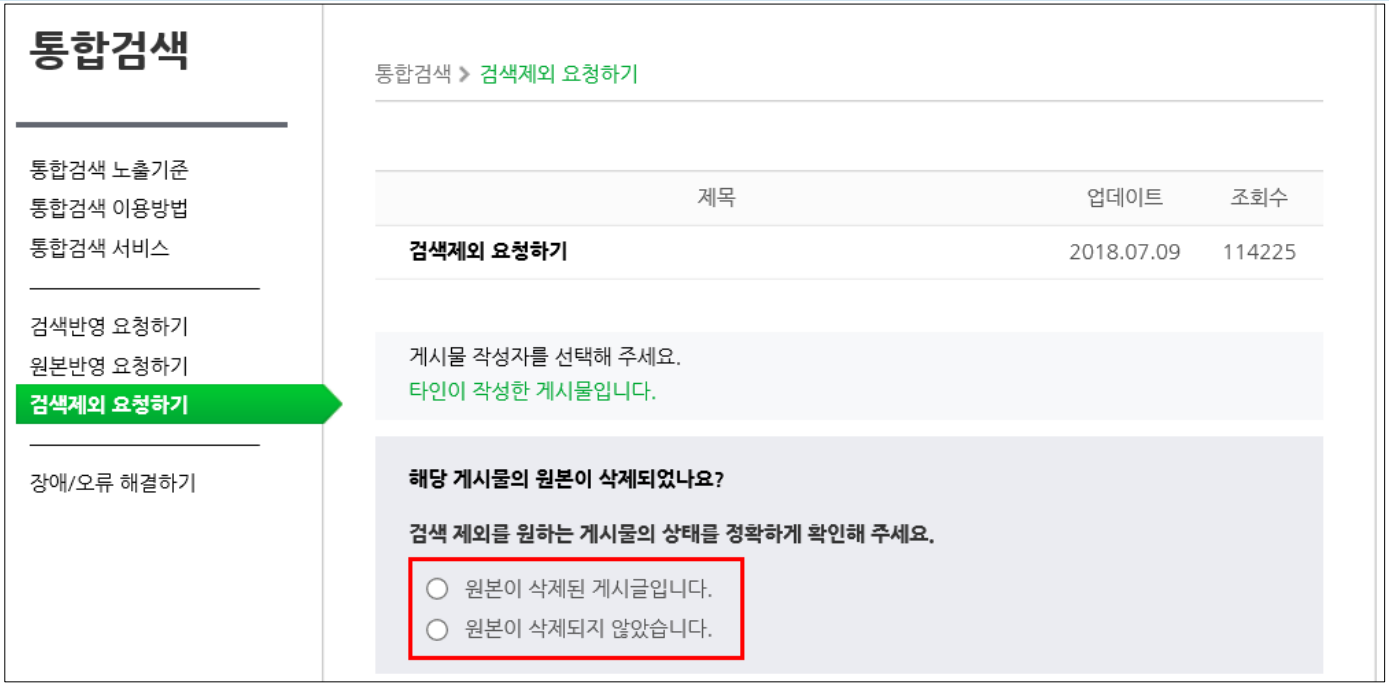
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 네이버 저장된 페이지 삭제 방법

⑥ 게시물 상태 선택

원본 게시물 삭제 후 캐쉬페이지 삭제 요청 하는 편이 좋고, 원본 게시물을 삭제하지 않고 캐쉬페이지 삭제 시 재노출 가능성 있음

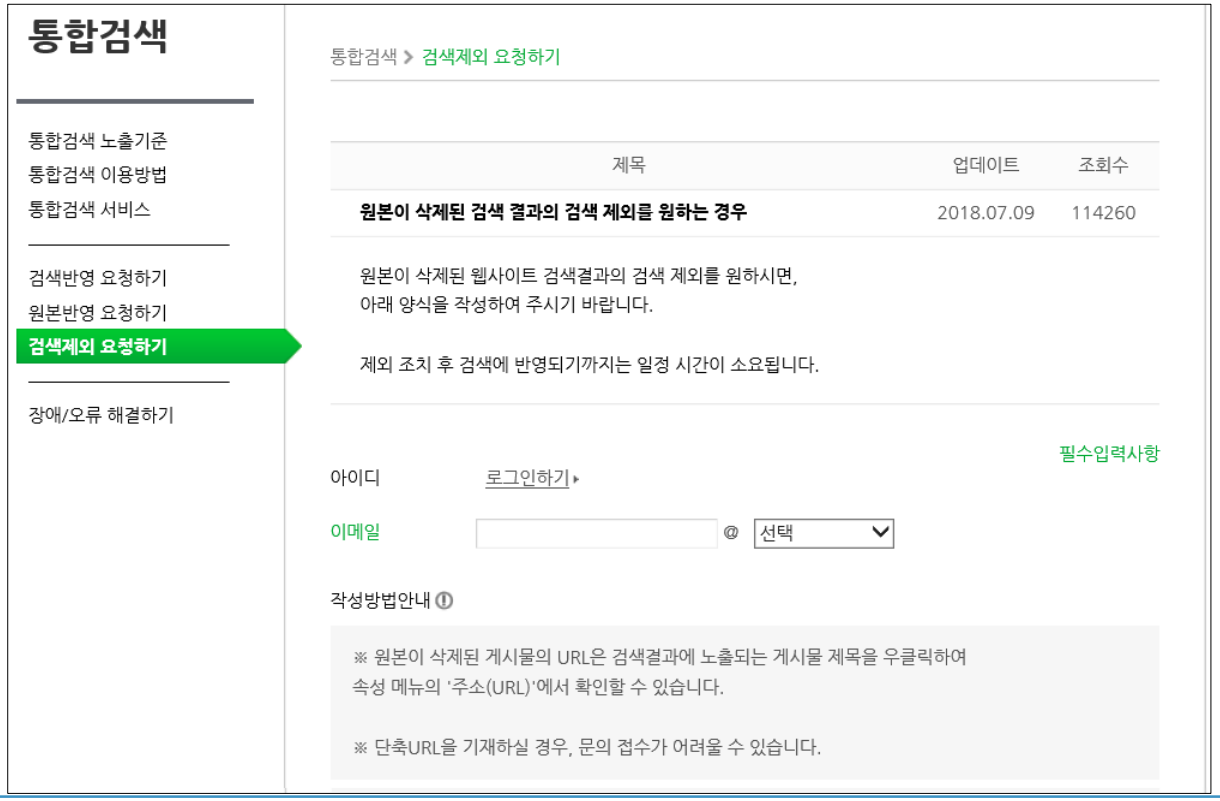


3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

▪ 네이버 저장된 페이지 삭제 방법

⑦ 신청자 정보 입력 및 신청완료



3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 네이버 저장된 페이지 삭제 방법

⑦ 신청자 정보 입력 및 신청완료

3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

▪ 네이버 저장된 페이지 삭제 방법

⑦ 신청자 정보 입력 및 신청완료

마지막으로 이메일, 삭제할 게시물 URL, 개인정보 수집동의 등 상세정보를 입력하여 캐쉬페이지 삭제 요청

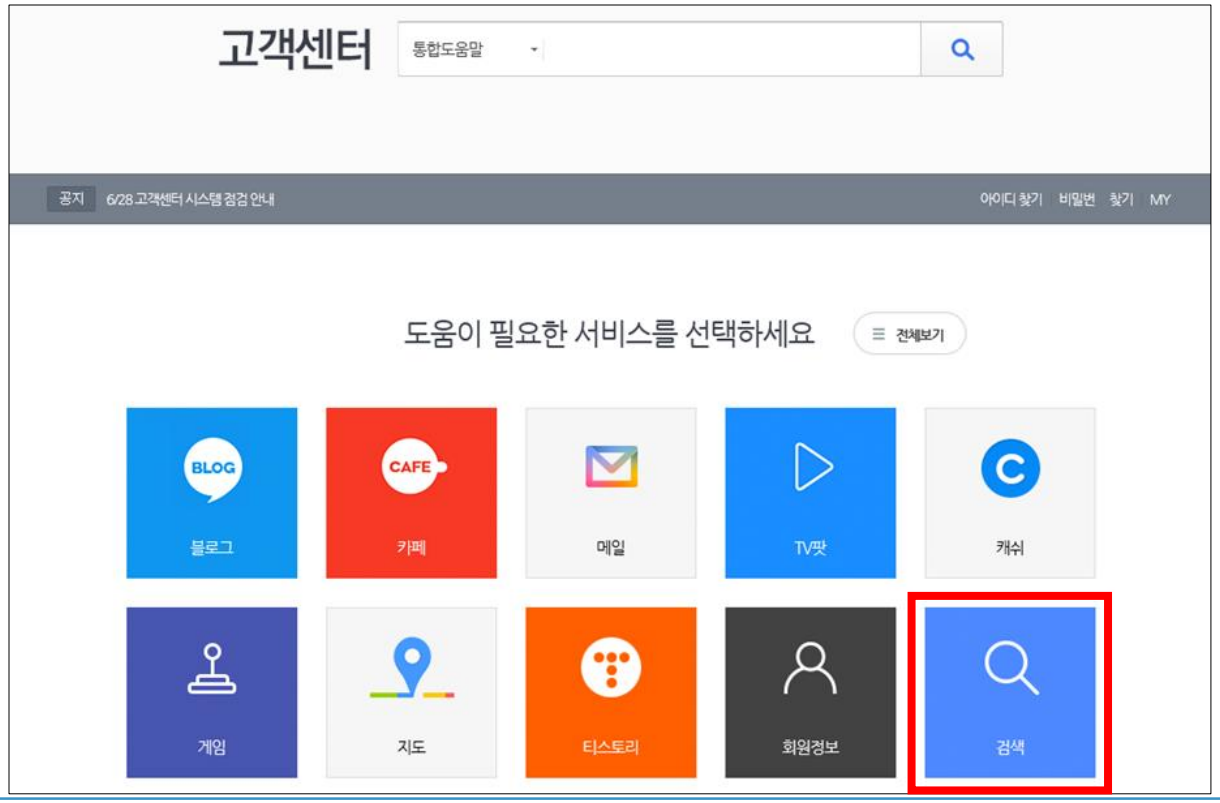
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

① 다음 고객센터

"검색" 탭 접속

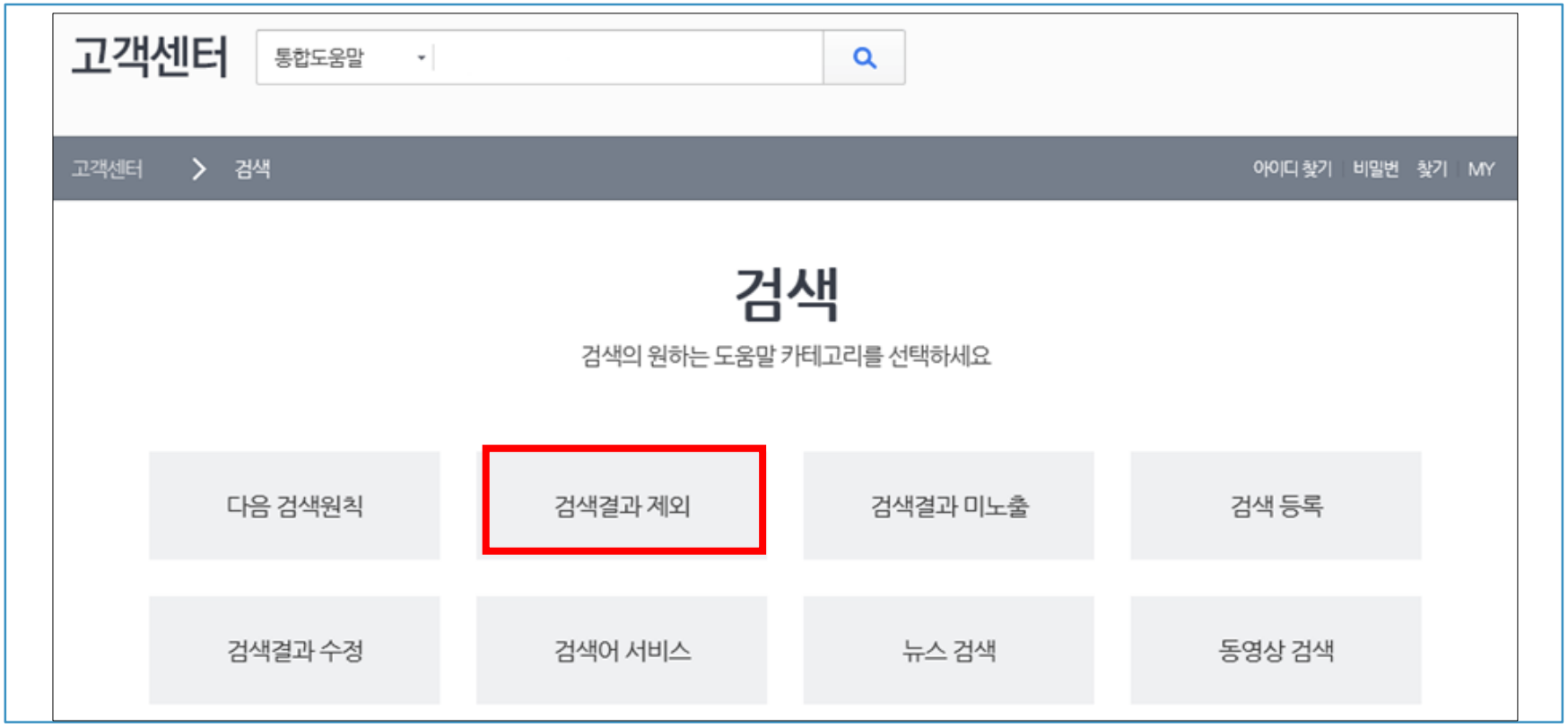


3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

② 검색결과 제외 선택



3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

③ 검색결과 제외 신청 선택

3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

④ 개인정보가 포함된 게시글이 검색되는데 삭제할 수 있나요 > Daum 고객센터 문의하기

개인정보가 포함된 게시글이 검색되는데 삭제할 수 있나요? ×

아래 내용을 기재하여 Daum 고객센터로 요청 시, 확인 후 검색에서 제외 처리될 수 있습니다.

Daum 고객센터 문의하기

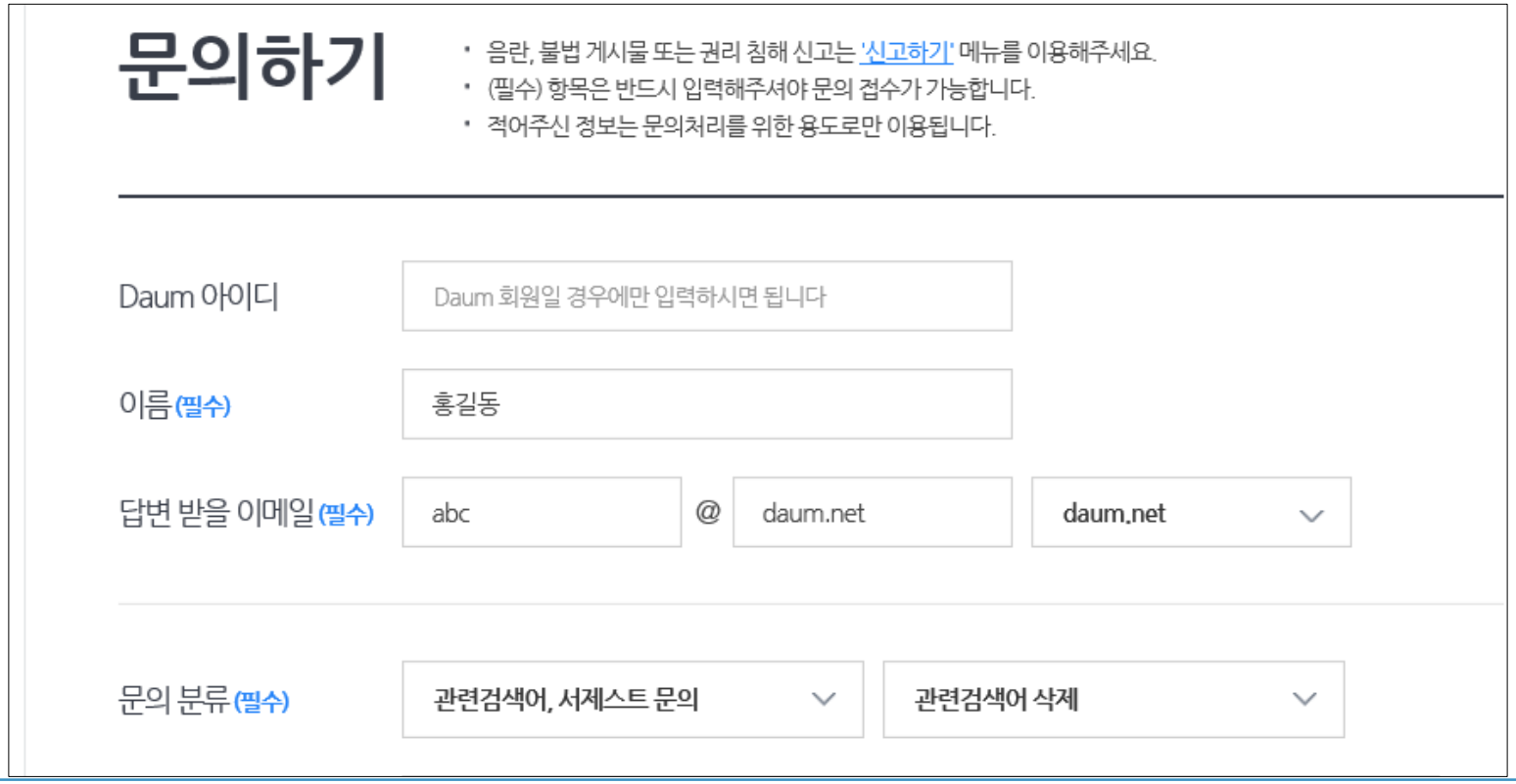
- 검색 URL
- 키워드
- 원문 URL
- 원문게시물 제목
- 삭제요청사유

3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

⑤ 제외신청 접수완료



3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

⑤ 제외신청 접수완료

제목 (필수)

개인정보 삭제요청

내용 (필수)

정확한 확인을 위해 아래 항목에 따라 내용을 작성해 주세요.

- 검색어 : 주민등록번호
- 삭제요청 관련검색어 : 주민등록번호
- 해당 URL : https://cs.daum.net/question/15.html
- 신고사유 : 개인정보노출

내용 확인을 위해 꼭 작성해 주세요.

- 요청인 성명 : 홍길동
- 인물과의 관계 : 본인
- 소속 : 한국인터넷진흥원
- 연락처 : 010-1234-5678

〈참고사항〉

권리침해 신고시 반드시 권리 증명 서류를 제출해주셔야 합니다.

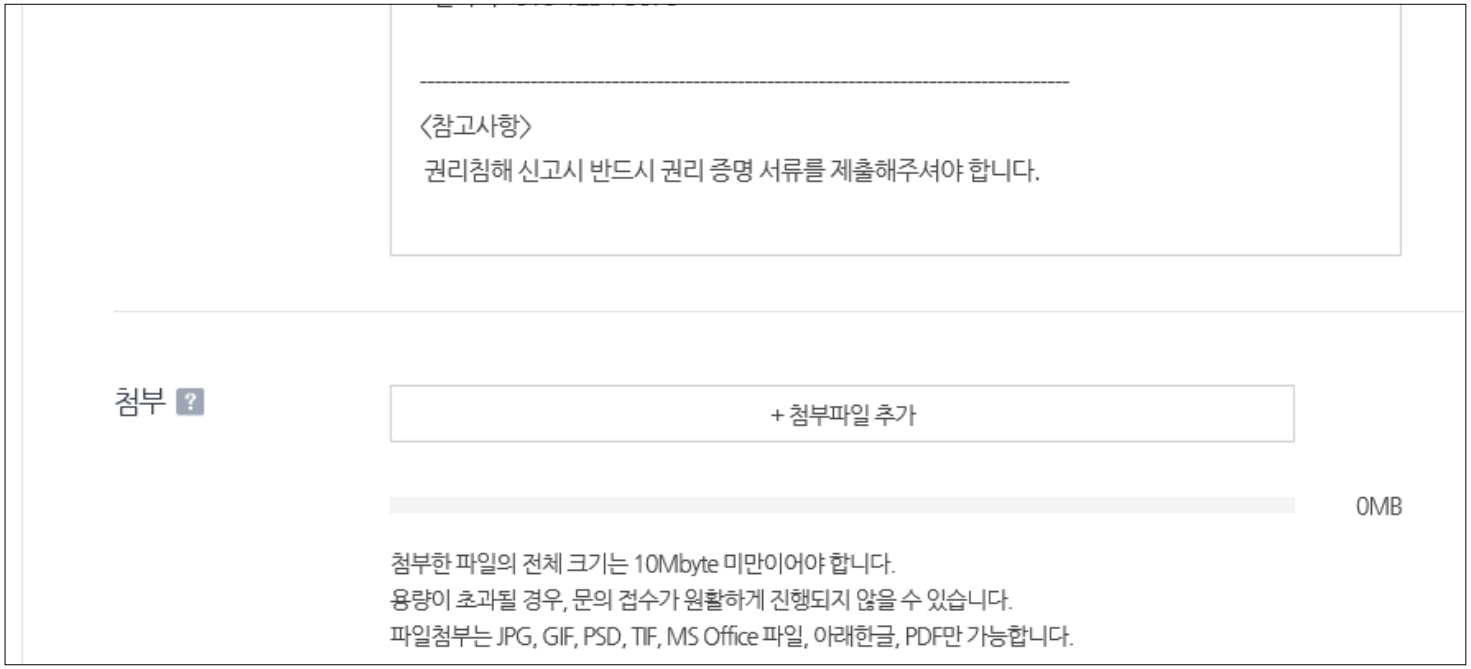
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 다음 저장된 페이지 삭제 방법

⑤ 제외신청 접수완료

필수항목(검색 URL, 키워드, 원문 URL, 원문게시물 제목, 삭제요청사유)을 작성하여 접수 시 개인정보 노출에 대한 삭제 요청 접수 후 처리



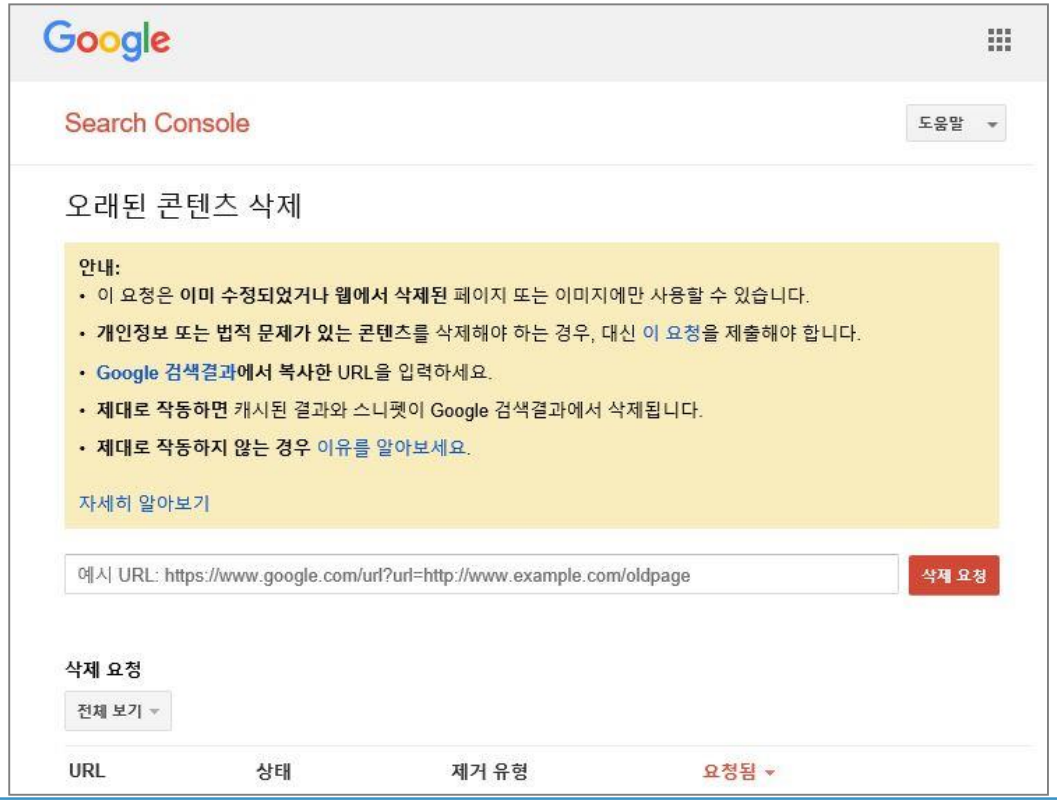
3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

▪ 구글 저장된 페이지 삭제 방법

① 구글 웹마스터 방문

삭제하려는 URL을 입력하고 '삭제 요청' 클릭



3. 검색엔진에 저장된 페이지 삭제

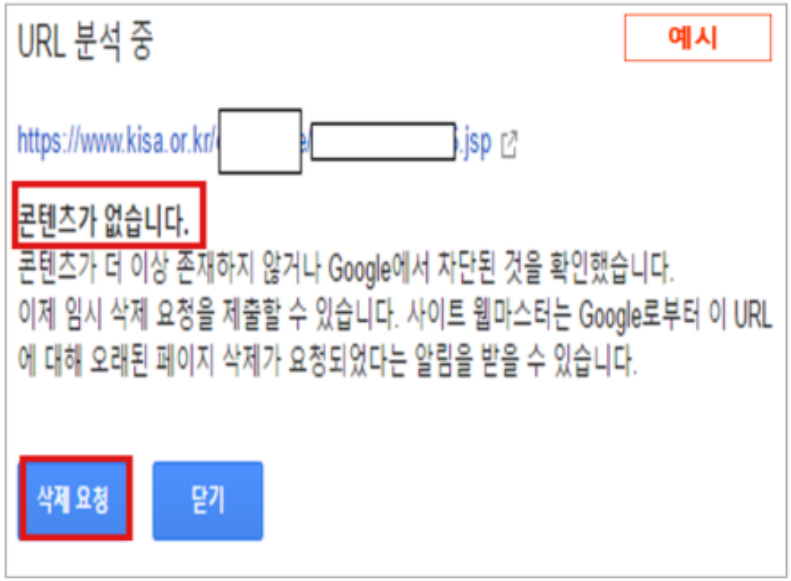
검색엔진 별 저장된 페이지 삭제 방법

- 구글 저장된 페이지 삭제 방법

② 화면 중 해당 되는 경우로 진행

<원본 정보가 삭제된 경우>

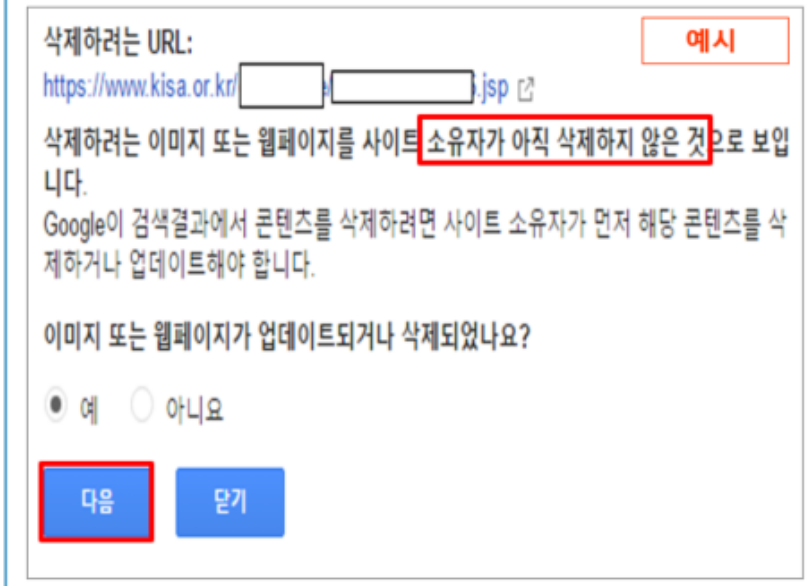
(원본 삭제, 캐시 미삭제)



'삭제 요청'을 클릭하면 삭제 요청 완료

<원본 정보가 남아있는 경우>

(원본, 캐시 모두 미삭제)



다음페이지로 이동

3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 구글 저장된 페이지 삭제 방법

③ 노출된 콘텐츠 입력

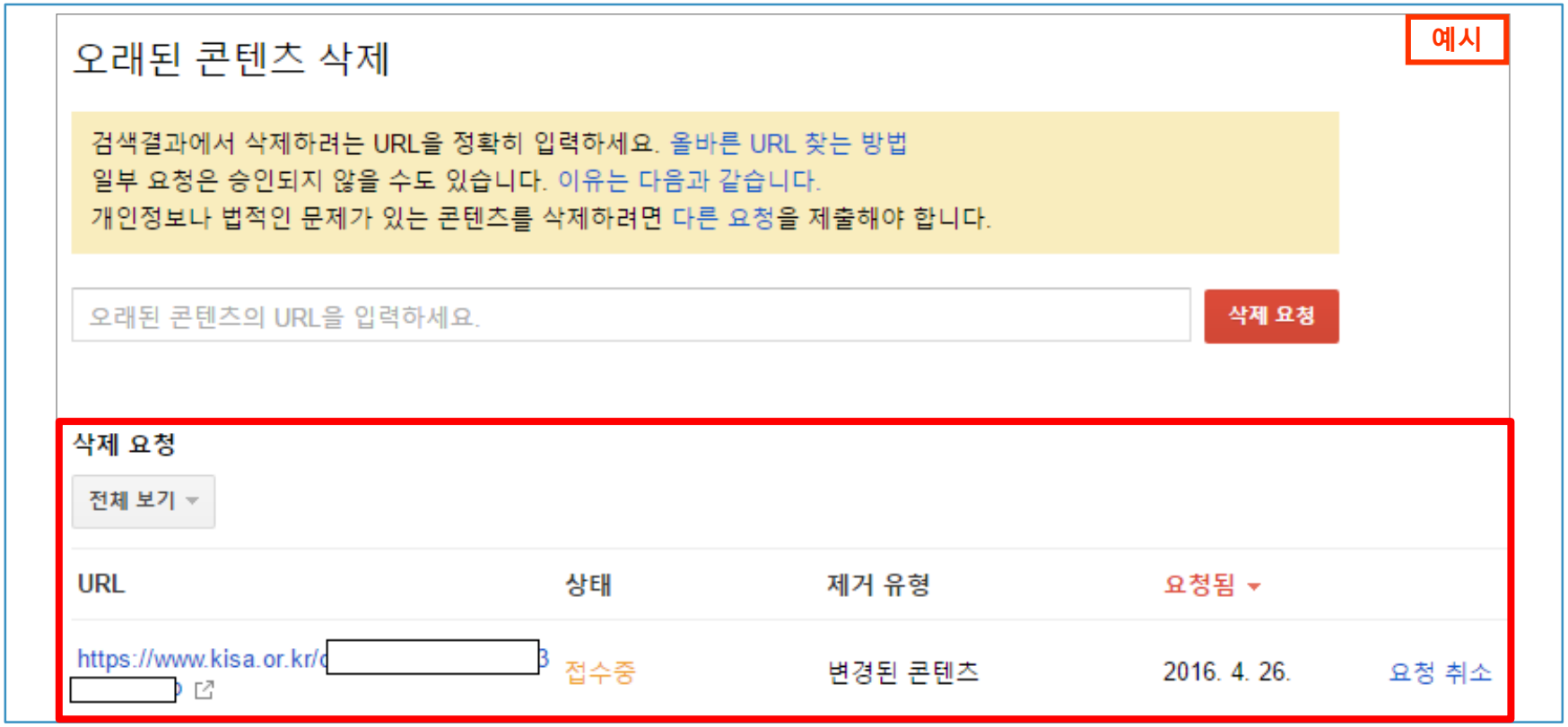
첫 번째 항목을 선택 후 캐시페이지에서 표시되는 내용의 일부 단어를 입력하고 '삭제 요청' 클릭

3. 검색엔진에 저장된 페이지 삭제

검색엔진 별 저장된 페이지 삭제 방법

- 구글 저장된 페이지 삭제 방법

④ 접수 상태 확인



Ⅳ. 개인정보 유출 사례 및 조치방안

1. 외부 공격
2. 고의(내부직원 유출)
3. 과실(담당자 업무관련)

개인정보 유출 사례 ①

외부 공격

1. 외부공격

DB 관리자페이지 공격으로 인한 유출

유출사례

- OO업체는 오프라인 매장에서 멤버십 회원 정보를 수집하여 회원관리시스템에 등록 후 구매 금액에 따라 적립금과 쿠폰 등 혜택을 제공함
- 신규 회원 등록 중 시스템 장애가 발생하여 담당부서에 확인 요청 후 시스템 담당자가 확인해보니 DB내 모든 데이터가 삭제되어 있었음
- 내부조사결과 해커가 관리자페이지를 통해 개인정보를 유출한 후 원본 데이터를 삭제하고 개인정보를 대가로 비트코인을 요구하는 메시지를 남겼음

1. 외부공격

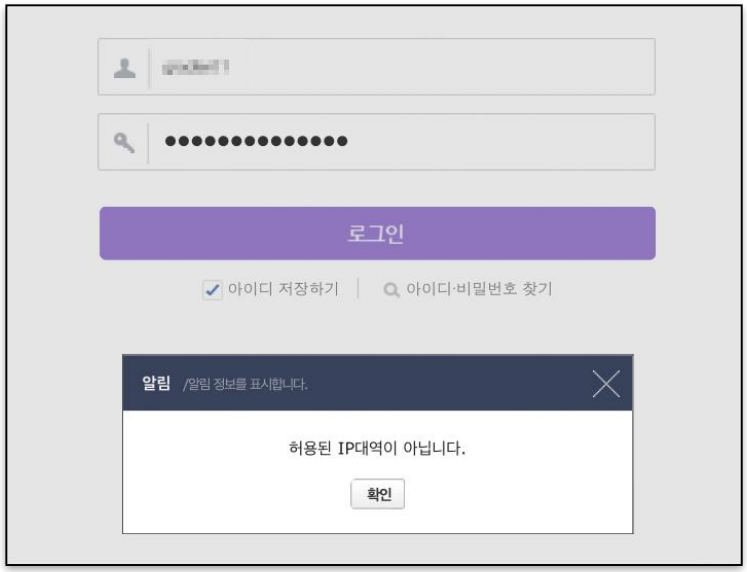
DB 관리자페이지 공격으로 인한 유출

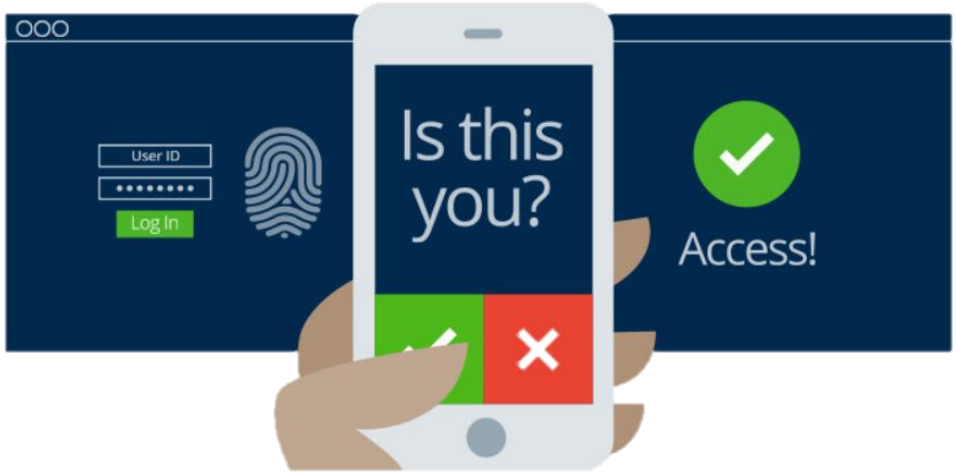
조치방법

- 접속권한을 IP주소, 포트, MAC주소 등으로 제한하여 인가받지 않은 접근을 제한
- 정보통신망을 통해 외부에서 시스템에 접속 시 가상사설망(VPN) 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용
- 개인정보취급자의 계정 설정 시 안전한 비밀번호 사용 (영문,특수문자,숫자로 최소8자리 이상)

  * 특히 DB에 접속하는 DB관리자의 비밀번호는 변경 주기를 짧게 하는 등 하고 강화된 안전조치를 적용 *

  * ID:root, PW:root 와 같이 취약한 비밀번호는 사용하지 않는다





1. 외부공격

SQL인젝션 공격으로 인한 개인정보 유출

유출사례

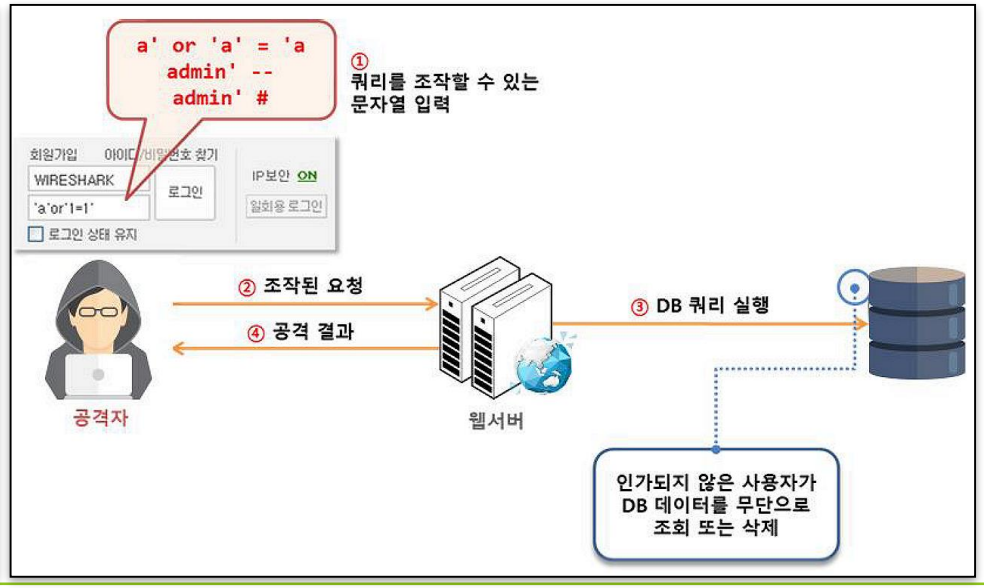
- B사업자는 자사 홈페이지 회원정보로 추정되는 개인정보가 해외 불법 해킹사이트에 게시되어 있다는 사실을 제보 받음
- 불법 해킹사이트에 게시된 개인정보를 현재 서버에 저장된 개인정보와 비교하여 자사의 개인정보와 일치함을 확인함
- 유출된 개인정보로 유출 시점을 추정하여, 해당 시점 웹서버 로그를 분석한 결과 SQL 인젝션 공격으로 시스템이 해킹당해 개인정보가 유출되었음을 알게됨

[해킹]흔한해킹수법'SQL인젝션'에뚫려

홈페이지에 악의적 시스템 명령 숨겨

= 의

홈페이지는 웹해킹에 많이 이용되는 'SQL 인젝션(Injection) 공격'을 당해 뚫린 것으로 드러났다.13일 보안 업계에 따르면 SQL 인젝션은 홈페이지에 악의적인 시스템 명령을숨겨놓고 방문자를 감염시키는 해킹 수법이다.해커들은 로그인인증을 우회해 데이터베이스에 있는 회원 아이디와패스워드 등의 개인정보를 빼돌릴 수 있다.

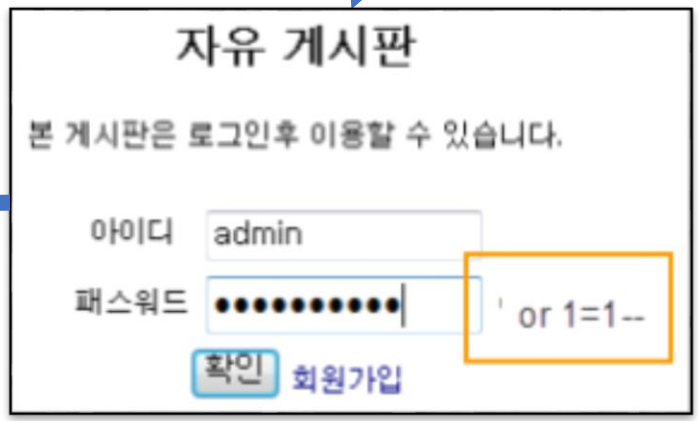


[참고] SQL Injection

웹 응용 프로그램에 강제로 SQL구문을 삽입하여 사용자 인증을
우회함으로써, 내부 DB서버의 데이터를 유출 및 변조

select id from [table_name]

where id='admin' and pw=''



1. 외부공격

SQL인젝션 공격으로 인한 개인정보 유출

조치방법

- 웹방화벽, IDS등을 구축·운영하여 SQL인젝션 공격 탐지 및 차단
- DB쿼리문에 들어가는 입력데이터 검증
  → SQL 쿼리문 및 특수문자가 있을 경우 필터링 및 치환하도록 적용
- DB사용자의 계정 권한을 제한하고, 웹어플리케이션 실행에 필요한 최소한의 권한만 부여

로그인 인증 우회에 대한 예시(사용자 인증 우회 점검)

1 OR 1=1	1' OR '1'='1	'1 OR '1=1--	' or 1=1;--
' or 1=1--	A' or 'A'='A	' or 1=1--	' or''='
'or'='or'	'or 'a'='a--	" or "a"="a	" or 1=1--
") or ("a"="a	') or('a'='a	"='	' and [??] and
'unusual'	' OR 'text'=	) or (1=1	Or 'a='a
N'text'	' OR 2>1	'some'+'thing'	' OR'something'=
' OR 'text'>'t'	" or 1=1--	like 'some%'	' OR 'something'
Aa' OR 'A'='A	' or 'a'='a	'or'='	'having 1=1--
or 1=1--	') or ('a'='a	1' or 1=1--	' or 'a'='a

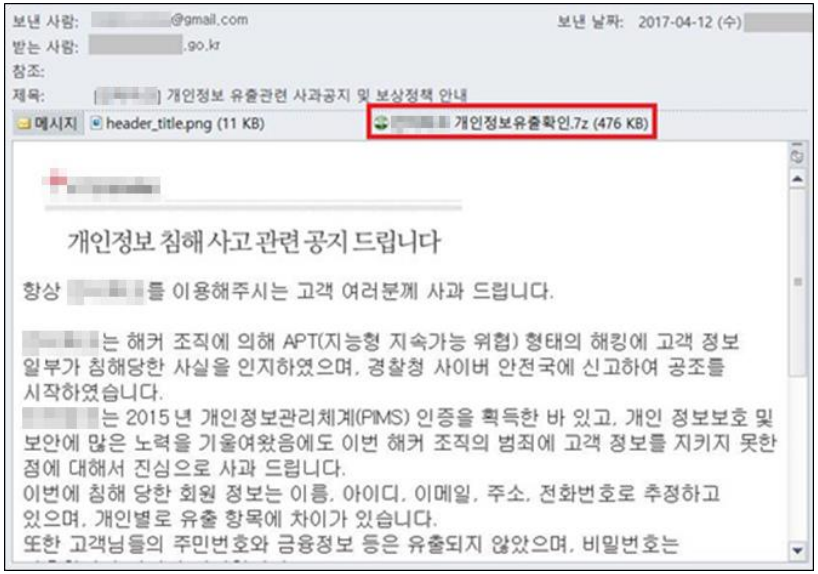
```
query("SELECT * FROM user WHERE id=:id", $bind["id"]=$_GET['id'])
```

1. 외부공격

지능형지속공격(APT, Advanced Persistent Threat)

유출사례

- OO업체 직원 이모씨는 업무용 PC에서 개인 이메일을 확인하던 중, 해커가 타 회사를 사칭하여 발송한 이메일을 열람함
- 이모씨는 별다른 의심없이 메일에 첨부된 파일을 실행하였고, 해커가 숨겨놓은 악성코드가 PC에 자동으로 설치되어 이모씨의 PC를 감염시킴
- 해커는 키로깅을 통해 개인정보처리시스템 계정을 획득한 뒤, 이모씨가 퇴근한 후 원격으로 PC를 제어하여 시스템을 통해 대량의 개인정보를 유출함


보낸 사람: @gmail.com
보낸 날짜: 2017-04-12 (수)
받는 사람: .go.kr
참조:
제목: [ ] 개인정보 유출관련 사과공지 및 보상정책 안내
메시지 header_title.png (11 KB) 개인정보유출확인.7z (476 KB)

개인정보 침해사고 관련 공지 드립니다

항상 를 이용해주시는 고객 여러분께 사과 드립니다.

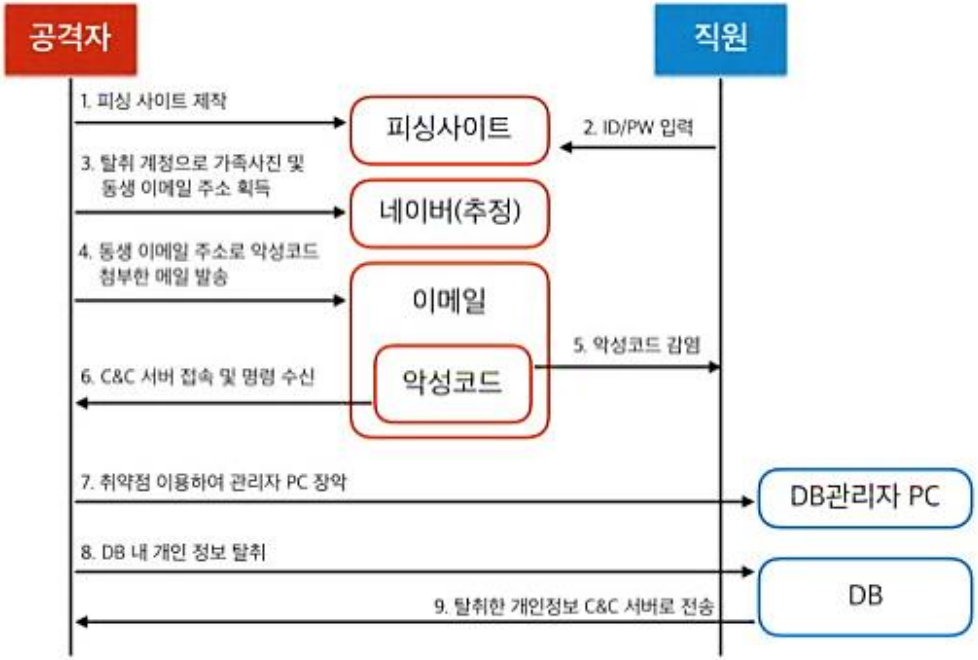
는 해커 조직에 의해 APT(지능형 지속가능 위협) 형태의 해킹에 고객 정보 일부가 침해당한 사실을 인지하였으며, 경찰청 사이버 안전국에 신고하여 공조를 시작하였습니다.
는 2015년 개인정보관리체계(PIMS) 인증을 획득한 바 있고, 개인 정보보호 및 보안에 많은 노력을 기울여왔음에도 이번 해커 조직의 범죄에 고객 정보를 지키지 못한 점에 대해서 진심으로 사과 드립니다.
이번에 침해 당한 회원 정보는 이름, 아이디, 이메일, 주소, 전화번호로 추정하고 있으며, 개인별로 유출 항목에 차이가 있습니다.
또한 고객님들의 주민번호와 금융정보 등은 유출되지 않았으며, 비밀번호는

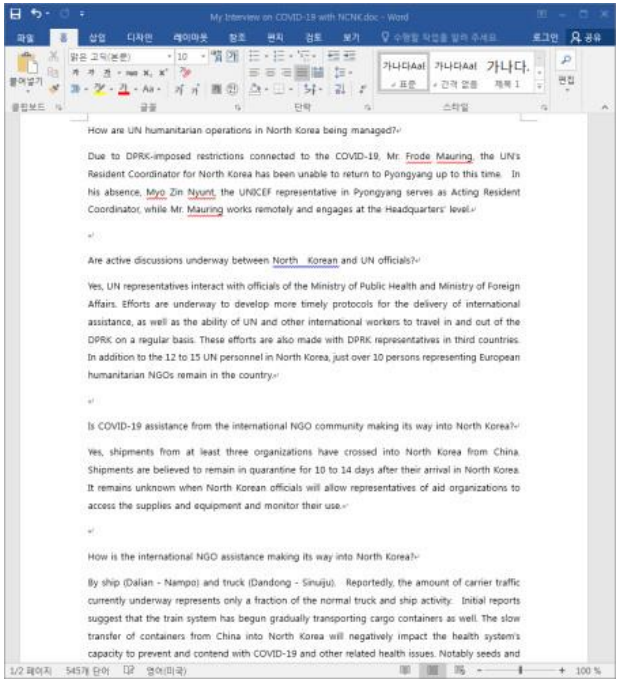
1. 외부공격

지능형지속공격(APT, Advanced Persistent Threat)

조치방법

- APT공격 대응 솔루션 도입·운영 및 스팸메일과 첨부파일 필터링 및 차단
- 의심스러운 이메일 열람 및 이메일내 링크 주소 클릭, 첨부파일 실행 등 금지
- 정기 보안교육과 모의훈련을 통해 취급자의 인식 강화





이스트시큐리티, '코로나19 상황 인터뷰 문서' 사칭 APT 공격 주의_디지털데일리뉴스

개인정보 유출 사례 ②

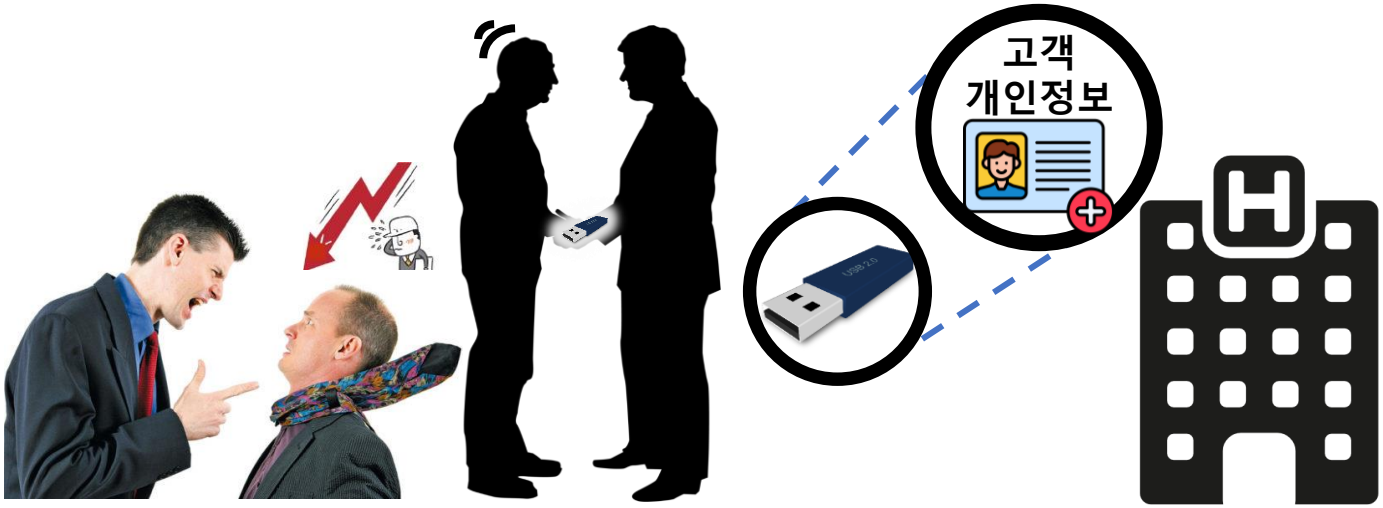
고의(내부직원 유출)

2. 고의(내부직원 유출)

업무 담당자가 지인의 부탁을 받고 고객정보 유출

유출사례

- OO호텔 업무 담당자 김모씨는 평소 알고 지내던 박모씨의 보험 영업 실적이 좋지 않자, 자신의 부하직원 윤모씨에게 지시하여 OO호텔 멤버십 회원의 개인정보(이름, 연락처) 2천건을 엑셀파일로 다운로드 한 후 USB에 저장하여 박모씨에게 제공함
- OO호텔의 개인정보 담당자는 매월 진행하는 접속기록 점검 중 특정일에 대량의 개인정보가 여러 차례 다운로드 된 것을 수상히 여겨 내부조사한 결과
  윤모씨가 상사인 김모씨의 지시를 받아 개인정보를 USB에 저장 후 제공한 사실을 알게됨



2. 고의(내부직원 유출)

업무 담당자가 지인의 부탁을 받고 고객정보 유출

조치방법

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

개인정보취급자 교육

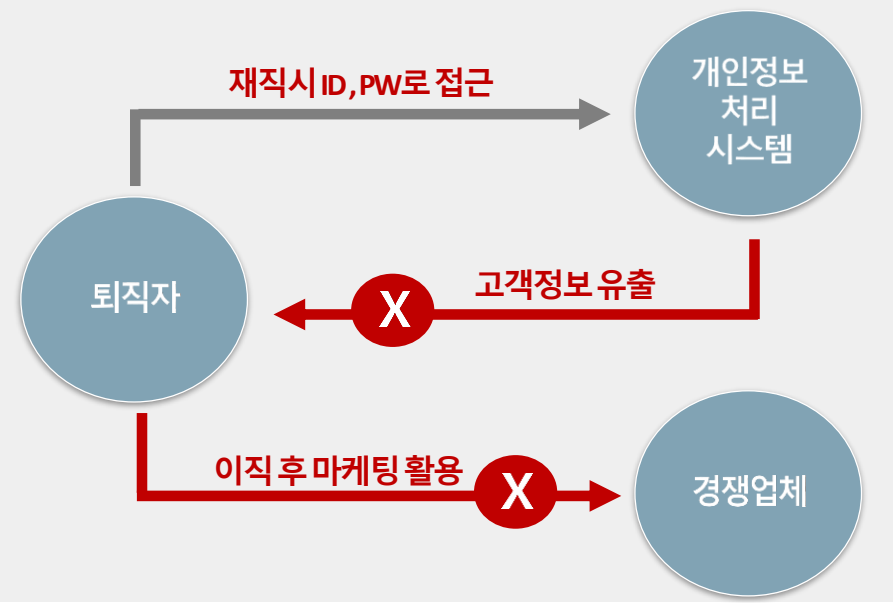
시건장치가 있는 캐비넷

2. 고의(내부직원 유출)

퇴직한 직원이 개인정보처리시스템에서 개인정보 유출

유출사례

- OO업체는 개인정보처리시스템을 통해 방문한 고객의 개인정보를 처리하고 있으나, 직원들의 잦은 퇴직으로 업무 편의상 계정을 공용으로 사용하고 있음
- OO업체에서 근무하였던 이모씨는 경쟁업체의 스카우트 제의를 받아 퇴사하였으나, 퇴사 이후에도 과거 사용하던 계정으로 시스템에 접근 가능한 것을 인지함
- 이모씨는 경쟁업체로 이직 후 OO업체의 시스템에 접속하여 고객의 개인정보 전체를 엑셀로 다운로드 받은 뒤 자신의 영업 실적을 위해 홍보문자 발송함



2. 고의(내부직원 유출)

퇴직한 직원이 개인정보처리시스템에서 개인정보 유출

조치방법

- 개인정보취급자의 계정을 공유하여 사용하지 말고, 취급자 별로 계정을 부여
- 전보, 퇴직 등 인사이동이 발생하였을 경우 지체없이 시스템 접근권한을 변경·말소
- 퇴직 점검표에 사용자계정 말소 항목을 반영하여 계정 말소 여부에 대해 확인 절차 마련
- 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여
- 내부관리계획에 개인정보 다운로드 기준을 마련하고,
  접속기록을 매월 점검하여 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

개인정보 유출 사례 ③

과실(담당자 업무관련)

3. 과실(담당자 업무 관련)

업무 담당자 행사 안내메일 단체발송

유출사례

- OO업체는 자사의 홈페이지 회원대상으로 신제품 체험 행사를 기획함
- 업무 담당자 박모씨는 생각보다 낮은 참석 응답률로 인해, 더 많은 고객이 참석할 수 있도록 회원 전체를 대상으로 행사 안내메일을 발송함
- 박모씨는 이메일 발송 후 고객 민원 전화를 통해 자신이 이메일을 단체발송하여 고객의 성명, 이메일주소가 유출됨을 인지함

단체 메일 발송할 때 '아차'하면 개인정보 '유출'된다

단체 메일(동보 메일) 발송시 반드시 '숨은 참조'나 '개별발송' 기능으로 수신자 정보 숨겨야
KISA, 2018 주요 개인정보 침해사고의 하나로 동보 메일 선택

최근 대량 메일을 발송하면서 메일을 받는 수신자를 별도의 '숨은 참조'나 '개별발송' 기능으로 숨기지 않아 이메일 등 개인정보가 유출되는 사고가 끊이질 않고 있다. 실제로 매일 여러 건의 보도자료를 받는 기자 역시도 이러한 개인정보 유출사고를 자주 겪을 정도로 꾸준하게 발생하지만, 이에 대한 관계자들의 개인정보보호 인식은 아직 바닥 수준이다.

3. 과실(담당자 업무 관련)

업무 담당자 행사 안내메일 단체발송

조치방법

- 외부로 발송하는 이메일의 경우 개별발송을 기본 옵션으로 지정
- 개인정보취급자 교육을 통해 이름, 이메일주소가 개인정보임을 숙지
- 이메일 개별발송 선택 시 개별발송 여부를 묻는 팝업창 게재 등 시스템 개선

Ⅴ. 개인정보 유출사고 조치 및 책임

1. 개인정보 유출 신고 방법
2. 개인정보 유출 통지 방법
3. 기준 및 처벌규정
4. 관련규정 및 조치기준

개인정보 유출 사고 조치 및 책임①

개인정보 유출 신고 방법

1. 개인정보 유출 신고 방법

관련 규정

- ✓ 개인정보가 유출되었음을 인지한 때에는 지체 없이 해당 정보주체에게 통지
- ✓ 피해 최소화를 위한 대책 마련 및 조치, 개인정보보호위원회/KISA에 신고 필요

* 개인정보처리자 : 5일 이내 통지, 1천건 이상 신고 / 정보통신제공자 : 24시간 이내 통지 및 신고

01 유출된 정보주체 개개인에게 지체없이 통지

→ 개인정보 보호법 제34조 제1항

| 시 한 | 유출되었음을 알게 되었을 경우 지체없이(5일 이내)

|통지항목| ① 유출된 개인정보의 항목

② 유출 시점과 그 경위

③ 피해 최소화를 위한 정보주체의 조치방법

④ 기관의 대응 조치 및 피해 구제 절차

⑤ 피해 신고 접수 담당부서 및 연락처

02 피해 최소화를 위한 대책 마련 및 필요한 조치 실시

→ 개인정보 보호법 제34조 제1항

| 접속 경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급조치 이행

| 긴급 조치 이행 등에 어려움이 있는 경우 전문기관에 기술 지원 요청

*피해 최소화 대책을 마련하지 않거나 필요한 긴급 조치를 하지 않은 경우 : 시정명령

03 1천 명 이상 유출된 경우 유출 통지 결과 신고

→ 개인정보 보호법 제34조 제3항

| 1천명 이상 유출된 경우 유출 통지 및 조치 결과를 지체 없이 개인정보보호위원회 또는 전문기관(한국인터넷진흥원)에 신고

* 개인정보보호법 제75조제2항제9호(3천만 원 이하의 과태료) 조치 결과를 신고하지 않은 자(개인정보보호위원회 또는 전문기관에 통지 결과 등을 신고하지 않은 경우)

04 1천명이상유출된경우에는추가로홈페이지에공지

→ 개인정보 보호법 시행령 제40조 제3항

| 1천명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재

* 홈페이지 등에 공지하지 않거나 7일 미만으로 게재하는 경우 : 시정명령

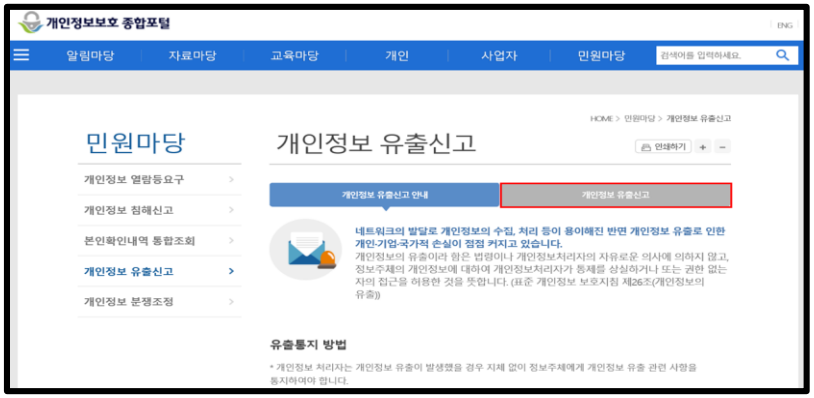
1. 개인정보 유출 신고 방법

개인정보 유출 신고 절차(공공기관 일반사업자)

1 개인정보보호 종합포털(www.privacy.go.kr) 접속

2 민원마당 내 '개인정보 유출신고' 클릭

3 개인정보 유출신고 안내사항 확인 후 작성



4 유출신고 작성예시

유출된 개인정보의 항목 및 규모 *	이름, 주소, 휴대전화 번호, 이메일, 주소 등 16만5000건의 개인정보 64 / 4000 byte
유출된 시점과 그 경위 *	내부직원이 어제 저녁 악성코드가 첨부된 이메일을 열람하고 악성코드에 감염되었고 (5.3 오후 16:38), 이메일을 열람한 내부직원의 PC를 경유하여 파일공유서버에 악성코드가 설치되면서(5.3 오후17:41), 파일공유서버에 연결 된 개인정보 취급자 PC의 262 / 4000 byte
유출피해 최소화 대책, 조치 및 결과	각 이용자들이 개인정보 유출여부를 확인할 수 있도록 조회사이트를 개설하였으며, 홈페이지 개인정보 유출 통지문을 통해 이용자들께 공지를 한 상태입니다. 또한 탈취한 개인정보를 이용한 보이스피싱/운영자사칭/이메일을 통한 악성코드 유포 253 / 4000 byte
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	1. 지능형 스팸차단서비스를 이용한 스팸 차단 2. 수신 스팸메일 적극 신고 3. 비밀번호 변경 등 90 / 4000 byte

1. 개인정보 유출 신고 방법

개인정보 유출 신고 절차(정보통신망서비스제공자)

1 온라인 개인정보보호 포털(www.i-privacy.kr) 접속

2 '개인정보 유출신고'-'개인정보 유출신고하기' 클릭

3 유형 선택 후 유출신고서 작성

4 유출신고 작성예시

개인정보 유출 사고 조치 및 책임②

개인정보 유출 통지 방법

2. 개인정보 유출 통지 방법

개인정보 유출통지 의무

(개인정보보호법 제34조 제1항)

|시한| 유출되었음을 알게 되었을 경우 **지체 없이 통지(통상 5일 이내)**

| 통 지 항 목 |

① 유출된 개인정보의 항목

② 유출 시점과 그 경위

③ 피해 최소화를 위한 정보주체의 조치방법

④ 기관의 대응 조치 및 피해 구제 절차

⑤ 피해 신고 접수 담당부서 및 연락처

| 통 지 방 법 |

① 통지는 서면 등의 방법으로 하여야 함

② **서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법을 이용한 개별적 통지** 방법이면 가능

③ 확인사실의 우선통지 (유출된 개인정보의 항목, 유출 시점 및 그 경위의 구체적인 내용을 확인하지 못한 경우 → 추후 확인되는 사항을 추가로 알릴 수 있음

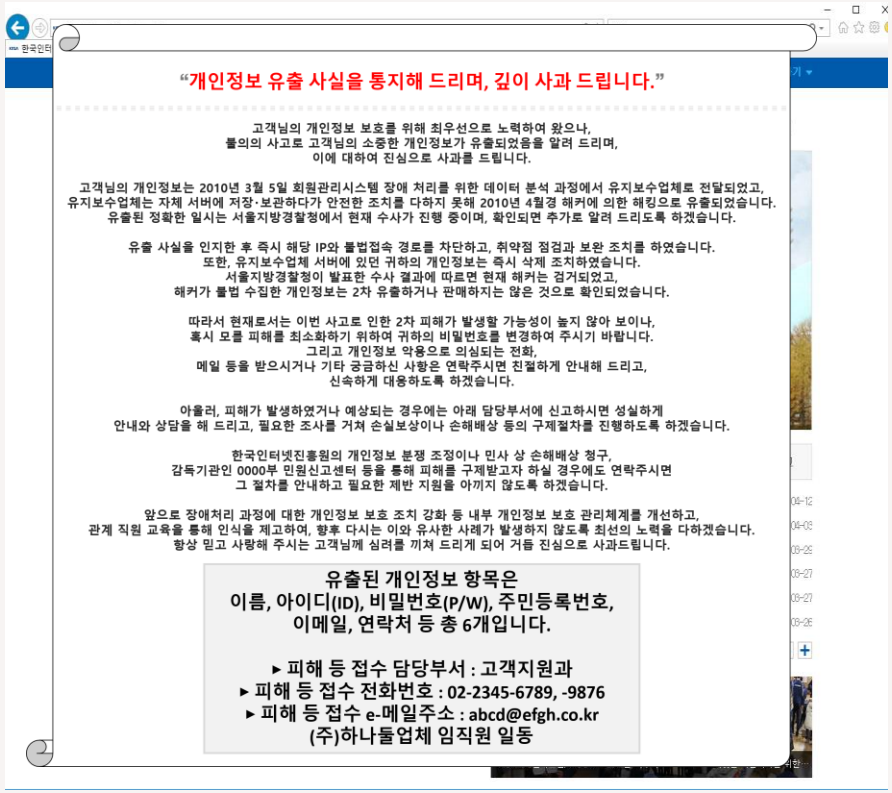
④ 개인정보가 유출되었음을 알게 되었을 때 통지 의무가 발생, 유출사실을 개인정보처리자가 인지한 시점에서 유출통지 의무가 발생

2. 개인정보 유출 통지 방법

홈페이지 게시

(개인정보보호법 시행령 제40조 제3항)

1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 **7일 이상 유출 통지사항을 게재하여야 함**



"개인정보 유출 사실을 통지해 드리며, 깊이 사과 드립니다."

고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나,
불의의 사고로 고객님의 소중한 개인정보가 유출되었음을 알려 드리며,
이에 대하여 진심으로 사과를 드립니다.

고객님의 개인정보는 2010년 3월 5일 회원관리시스템 장애 처리를 위한 데이터 분석 과정에서 유지보수업체로 전달되었고,
유지보수업체는 자체 서버에 저장·보관하다가 안전한 조치를 다하지 못해 2010년 4월경 해커에 의한 해킹으로 유출되었습니다.
유출된 정확한 일시는 서울지방경찰청에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.

유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다.
또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.
서울지방경찰청이 발표한 수사 결과에 따르면 현재 해커는 검거되었고,
해커가 불법 수집한 개인정보는 2차 유출하거나 판매하지는 않은 것으로 확인되었습니다.

따라서 현재로서는 이번 사고로 인한 2차 피해가 발생할 가능성이 높지 않아 보이나,
혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다.
그리고 개인정보 악용으로 의심되는 전화,
메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고,
신속하게 대응하도록 하겠습니다.

아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게
안내와 상담을 해 드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다.

한국인터넷진흥원의 개인정보 분쟁 조정이나 민사 상 손해배상 청구,
감독기관인 0000부 민원신고센터 등을 통해 피해를 구제받고자 하실 경우에도 연락주시면
그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.

앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고,
관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.
항상 믿고 사랑해 주시는 고객님께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.

유출된 개인정보 항목은
이름, 아이디(ID), 비밀번호(P/W), 주민등록번호,
이메일, 연락처 등 총 6개입니다.

▸ 피해 등 접수 담당부서 : 고객지원과
▸ 피해 등 접수 전화번호 : 02-2345-6789, -9876
▸ 피해 등 접수 e-메일주소 : abcd@efgh.co.kr
(주)하나둘업체 임직원 일동

|통지사항|

① 유출된 개인정보의 항목

② 유출 시점과 그 경위

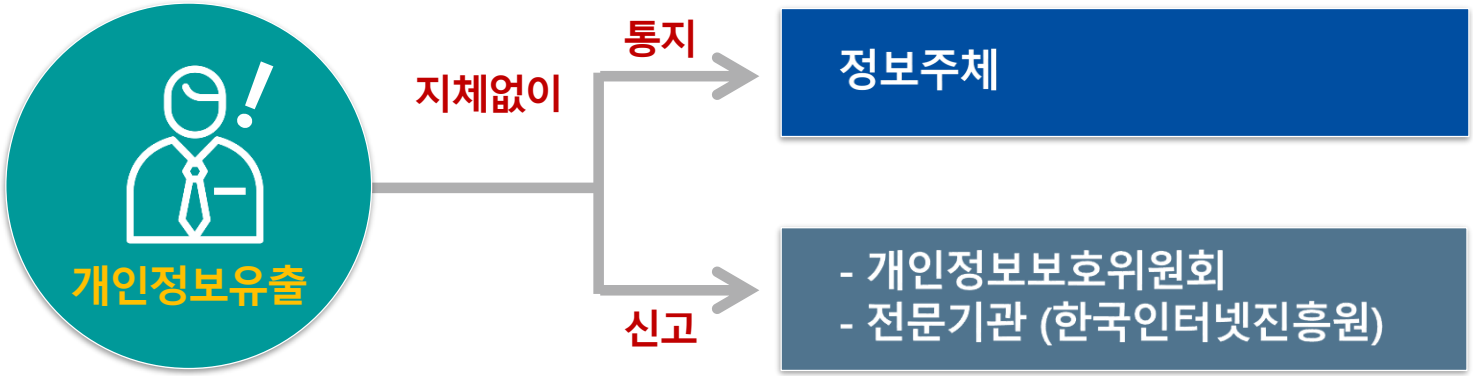
③ 피해 최소화를 위한 정보주체의 조치방법

④ 기관의 대응 조치 및 피해 구제 절차

⑤ 피해 신고 접수 담당부서 및 연락처

2. 개인정보 유출 통지 방법

유출통지 방법



통지방법	신고방법
통지대상	1건이라도 개인정보 유출 시, 정보주체에게 유출관련 사실을 통지
통지시기	5일 이내(개인정보보호법), 24시간 이내(정보통신망법)
통지방법	개별 통지 - 서면, 전자우편, 전화, 팩스, 문자전송 등 ※ 1천명 이상의 개인정보가 유출된 경우, 서면 등의 방법과 함께 인터넷 홈페이지에 7일 이상 게재(개인정보보호법)
통지내용	유출된 개인정보의 항목, 유출된 시점과 그 경위, 정보주체의 피해 최소화 방법, 사업자의 대응조치 및 피해구제 절차, 담당부서 및 연락처

2. 개인정보 유출 통지 방법

개인정보 유출 통지 사례

○○를 믿고 아껴 주시는 회원 여러분

그동안 ○○은 회원님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나,
불의의 사고로 회원님의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.

(② 유출 시점과 그 경위)
3월초, 서울 경찰청 사이버수사대에서 개인정보 유출과 관련하여 관리실태를 점검 중에 유출 정황 발견됐으며 이후 내부 개발팀의 진단 결과, 회원님의 개인정보는 2018년 4월 1일 14시 40분경 해커에 의한 해킹으로 유출 된 것으로 밝혀졌습니다.

(① 유출된 개인정보의 항목)
유출된 개인정보 항목은 아이디(ID)와 이메일,
집 전화번호, 휴대폰번호, 생년월일 총 5개 입니다.

다행히, 개정된 정보통신망법에 따라 주민등록번호는 전량 폐기 후 수집하지 않고 있으며
비밀번호도 암호화로 보호돼 유출되지 않은 것으로 확인되었습니다.

2. 개인정보 유출 통지 방법

개인정보 유출 통지 사례

(④ 기관의 대응 조치)
○○는 유출 사실을 인지한 후 즉시 취약점 점검과 보완조치를 하였습니다. 한편, 전화번호 및 휴대폰번호는 개인정보암호화 작업으로 보안을 강화하였으며 웹 방화벽, IPS 장비를 이용해 현재도 강력한 보완유지에 힘쓰고있습니다.

(③ 피해 최소화를 위한 정보주체의 조치방법)
비밀번호는 유출되지 않았지만 혹시 발생할지 모를 타 웹사이트에서의 2차 피해를 방지하기 위하여 번거로우시더라도 고객님께서는 현재 사용하시는 비밀번호를 변경하여 주시기 바랍니다. 또한 웹사이트에서 사용하고 계시는 동일한 아이디나 비밀번호의 경우, 해당 웹사이트에 방문하셔서 비밀번호를 변경하시는 것이 안전함을 알려 드립니다.

(④ 피해 구제 절차)
아울러 피해가 발생하거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해드리겠습니다. 앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.

2. 개인정보 유출 통지 방법

개인정보 유출 통지 사례

뜻하지 않게 개인 정보가 유출되어 회원 여러분의 심려를 끼쳐드린 점에 대해 거듭 진심으로 사과 드립니다.

(⑤ 피해 신고 접수 담당부서 및 연락처)

■ 피해 등 접수 담당부서 : ○○ 운영팀
■ 피해 등 접수 전화번호 : 02-2164-1004
■ 피해 등 접수 E-메일주소 : ANGEL@GOD.COM

2. 개인정보 유출 통지 방법

유출통지 방법

Question

10만명 개인정보 유출된 상황

개인정보처리자 A

연락가능한 개인정보 항목
1. 핸드폰번호, 2. 이메일주소

1차 유출통지 : 이메일주소를 통해 메일발송
(10만명중 4만건은 반송)

2차 유출통지 : 핸드폰번호를 통해 SMS 발송
(4만명 중 2만건은 반송)

개인정보처리자 B

연락가능한 개인정보 항목
1. 핸드폰번호, 2. 이메일주소, 3.집주소

1차 유출통지 : 이메일주소를 통해 메일 발송
(10만명중 4만건은 반송)

2차 유출통지 : 핸드폰번호를 통해 SMS 발송
(4만명 중 2만건은 반송)

Answer

A는 유출 통지 의무를 완료했다고 보여지나,
B는 2만명에 대해 유출통지하지 않음(집주소를 가지고 있었음에도)

개인정보 유출 사고 조치 및 책임 ③

기준 및 처벌규정

3. 기준 및 처벌규정

행정처분 흐름도

3. 기준 및 처벌규정

개인정보 유출을 막으려면? **안전성 확보 조치**

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. 기준 및 처벌규정

민사

제39조의 2 (법정손해배상의 청구)

제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실・도난・유출・위조・변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015. 7. 24.]

3. 기준 및 처벌규정

행정벌

고시의 보호조치 **의무 위반과 유출사이의 인과관계를 요구하지 않음**(다만 '관련성' 은 요구 됨)

➢ 과징금의 부과

개인정보보호법 제34조의 2

(제1항) **보호위원회는 개인정보처리자가 처리하는 주민등록번호가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과 · 징수할** 수 있다.

다만, 주민등록번호가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

개인정보보호법 제39조의15

(제1항) **보호위원회**는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 **정보통신서비스 제공자 등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.**

(제1항제5호) 이용자의 개인정보를 **분실·도난·유출·위조·변조 또는 훼손한 경우**로서 제29조의 **조치를 하지 아니한 경우**

개인정보의 보호조치

3. 기준 및 처벌규정

형사벌

제73조(벌칙)

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. <개정 2015. 7. 24., 2016. 3. 29., 2020 2. 4..>

1. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실・도난・유출・위조・변조 또는 훼손당한 자

1의2. 제21조제1항을 위반하여 개인정보를 파기하지 아니한 정보통신서비스 제공자등

2. 제36조제2항을 위반하여 정정・삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자

3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

개인정보 유출 사고 조치 및 책임 ④

관련기준 및 조치기준

4. 관련규정 및 조치기준

근거 법령

① 개인정보 최소 수집 및 파기

② 인터넷 게시 전에 다시 한번 문서/홈페이지 확인

③ 관리자페이지는 반드시 보안설정

④ 주기적 점검(내부, 외부)은 필수

개인정보보호법 제29조(안전조치 의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

4. 관련규정 및 조치기준

내부 관리계획의 수립과 시행(제 4조)

개인정보보호 내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육
4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지
9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립 · 시행

12. 위험도 분석 및 대응방안 마련
13. 재해 · 재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

유형3만 해당

15. 그 밖에 개인정보 보호를 위해 필요한 사항

4. 관련규정 및 조치기준

내부 관리계획의 수립과 시행(제 4조) 위반사례

법령	위반사례
제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. (자료설명 : 내부 관리계획에 개인정보의 안전성 확보에 필요한 조치에 관한 사항 미 포함)	**개정 전** 개인정보의 안전성 확보에 필요한 조치에 관한 사항 **개정 후(2016.09.01 시행)** 개인정보의 안전조치에 관한 사항을 명확하게 명시 **개정 후 내부관리계획에 내용 추가** 1. 개인정보보호책임자(CPO) 지정 2. 개인정보보호 책임자 및 취급자의 역할과 책임 3. 취급자 교육 4. 접근권한 관리 5. 접근통제 6. 개인정보 암호화 7. 접속기록 보관 및 점검 8. 악성프로그램 방지 9. 물리적 안전조치 10. 개인정보 보호조직 구성·운영 11. 유출사고 대응계획 수립·시행 12. 위험도 분석 및 대응방안 마련 13. 재해·재난 대비 개인정보처리시스템의 물리적 안전조치 14. 개인정보처리 수탁자의 관리·감독 15. 그밖에 개인정보 보호를 위해 필요한 사항

4. 관련규정 및 조치기준

접근권한의 관리(제 5조)

① 개인정보처리시스템에 대한 접근권한은 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여

② 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 접근권한을 변경 또는 말소

③ 권한부여, 변경 또는 말소에 대한 내역을 기록하고, 최소3년간 보관

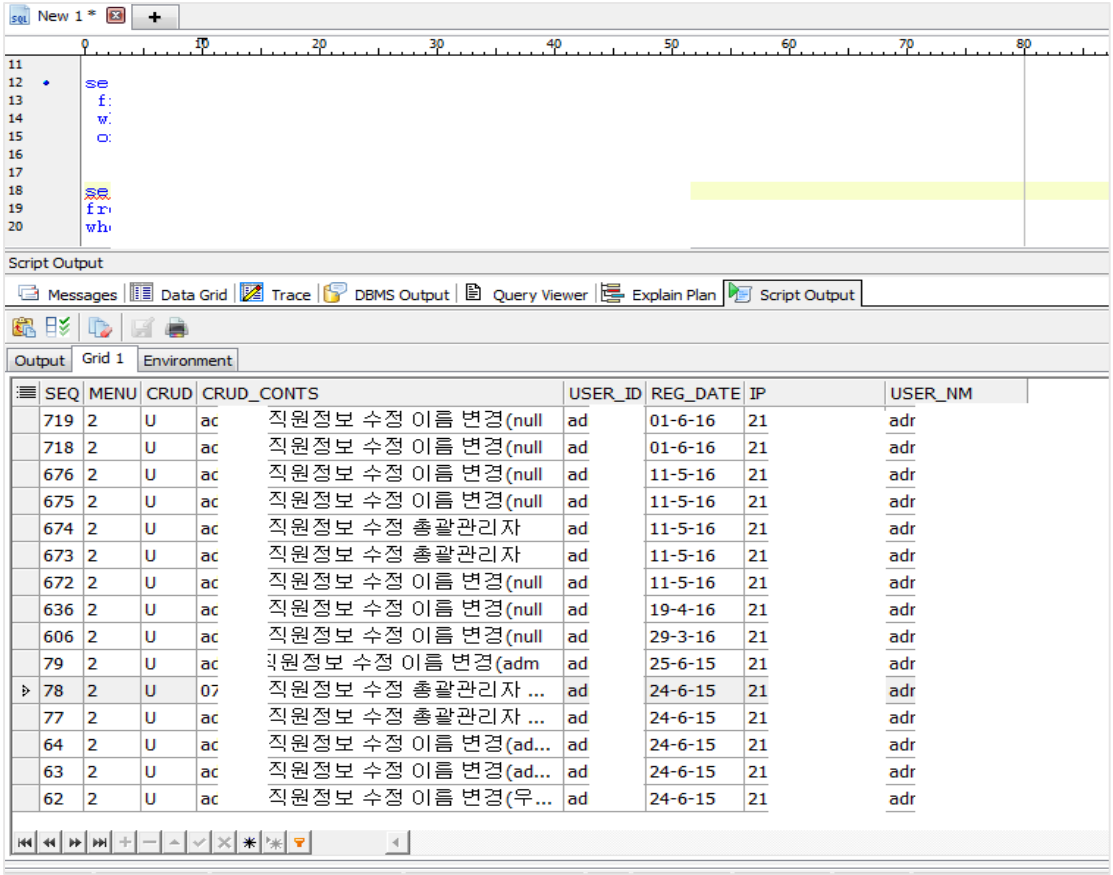
④ 사용자계정 발급 시 개인정보취급자 별로 발급하며, 다른 개인 정보취급자와 공유되지 않도록 함

⑤ 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용

⑥ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력 한 경우 접근 제한 등 필요한 기술적조치

4. 관련규정 및 조치기준

접근권한의 관리(제 5조) 위반사례

법령	위반사례
제5조(접근 권한의 관리) ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.	

New 1 *

Script Output

Messages | Data Grid | Trace | DBMS Output | Query Viewer | Explain Plan | Script Output

Output | Grid 1 | Environment

SEQ	MENU	CRUD	CRUD_CONTS	USER_ID	REG_DATE	IP	USER_NM
719	2	U	직원정보 수정 이름 변경(null	ad	01-6-16	21	adr
718	2	U	직원정보 수정 이름 변경(null	ad	01-6-16	21	adr
676	2	U	직원정보 수정 이름 변경(null	ad	11-5-16	21	adr
675	2	U	직원정보 수정 이름 변경(null	ad	11-5-16	21	adr
674	2	U	직원정보 수정 총괄관리자	ad	11-5-16	21	adr
673	2	U	직원정보 수정 총괄관리자	ad	11-5-16	21	adr
672	2	U	직원정보 수정 이름 변경(null	ad	11-5-16	21	adr
636	2	U	직원정보 수정 이름 변경(null	ad	19-4-16	21	adr
606	2	U	직원정보 수정 이름 변경(null	ad	29-3-16	21	adr
79	2	U	직원정보 수정 이름 변경(adm	ad	25-6-15	21	adr
78	2	U	직원정보 수정 총괄관리자 ...	ad	24-6-15	21	adr
77	2	U	직원정보 수정 총괄관리자 ...	ad	24-6-15	21	adr
64	2	U	직원정보 수정 이름 변경(ad...	ad	24-6-15	21	adr
63	2	U	직원정보 수정 이름 변경(ad...	ad	24-6-15	21	adr
62	2	U	직원정보 수정 이름 변경(우...	ad	24-6-15	21	adr

4. 관련규정 및 조치기준

접근통제(제6조)

① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 기본 조치

1. 접속 권한을 IP주소 등으로 제한 →인가 받지 않은 접근 제한
2 . 접속한 IP주소 등을 분석 → 법적인 개인정보 유출 시도 탐지 및 대응

→ 위 기능을 포함하여 조치해야 함

② 외부에서 개인정보처리시스템에 접속하려는 경우안전한 접속수단 또는 안전한 인증수단 적용

※ 가상사설망(VPN : Virtual Private Network) 또는 전용선 등

③ 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망이용 등을 통하여 개인정보가 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등 조치수행

4. 관련규정 및 조치기준

접근통제(제6조)

④ 인터넷 홈페이지를 통해 고유식별정보가 유출. 변조. 훼손되지 않도록 **연 1회 이상 취약점을 점검**하고 필요한 보완 조치 수행

⑤ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 **자동으로 시스템 접속이 차단되도록 해야 함**

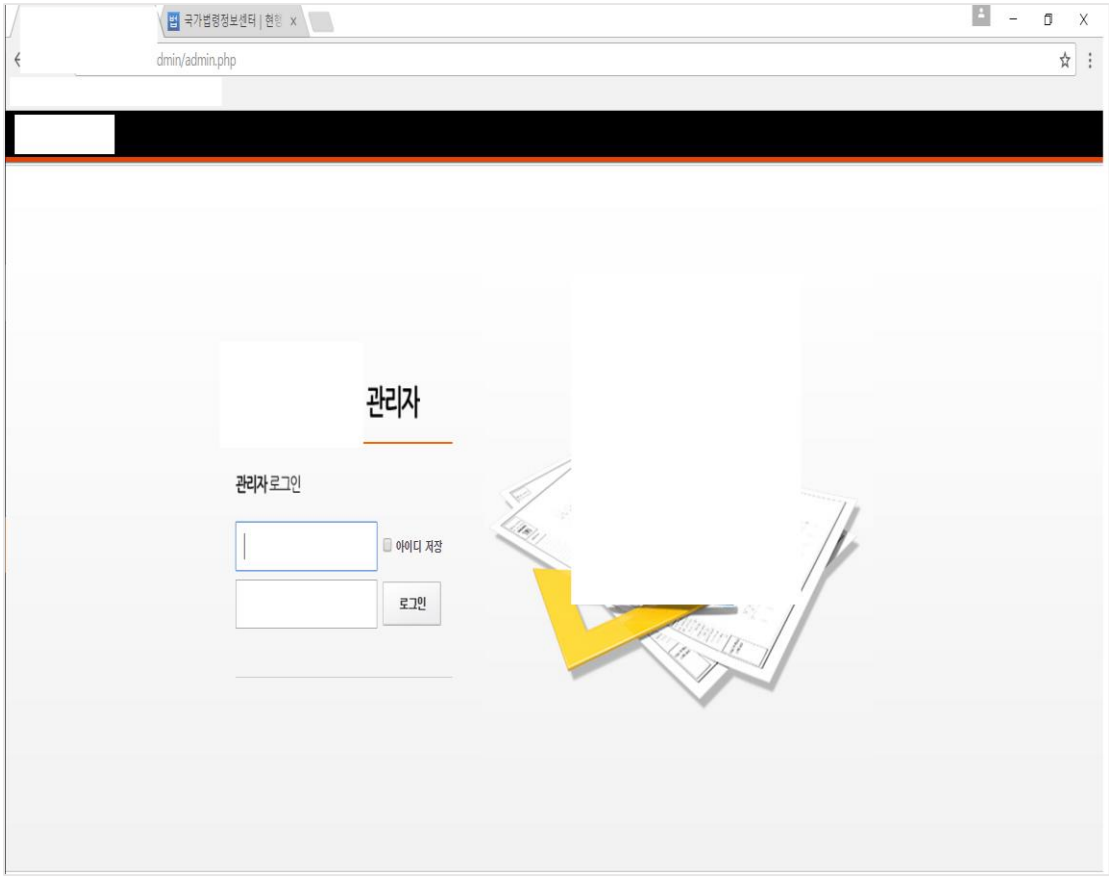
⑥ 별도의 개인정보처리시스템이 아닌 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우

- 제1항 적용 안함
- 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안 프로그램 등에서 제공하는 접근 통제 기능 이용 가능

⑦ 업무용 모바일 기기의 분실. 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 **기기에 비밀번호 설정 등의 보호조치**

4. 관련규정 및 조치기준

접근통제(제6조) 위반사례

법령	위반사례
제6조(접근통제) ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (자료설명 : 외부에서 개인정보처리시스템 접속 시 안전한 접속수단 및 인증수단을 사용하고 있지 않음)	

4. 관련규정 및 조치기준

개인정보 암호화(제7조)

<table>
<tr><th colspan="4">구분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망,
보조저장매체를 통한
송, 수신 시</td><td colspan="3">비밀번호,
바이오정보,
고유식별정보</td><td>암호화 송신</td></tr>
<tr><td rowspan="5">개인정보
처리시스템에
저장 시</td><td colspan="3">비밀번호</td><td>일방향(해쉬 함수) 암호화 저장</td></tr>
<tr><td colspan="3">바이오 정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="3">고유식별정보</td><td colspan="2">주민등록번호</td><td>암호화 저장</td></tr>
<tr><td rowspan="2">여권번호,
외국인 등록번호,
운전면허번호</td><td>인터넷 구간,
인터넷 구간과
내부망의 중간
지점(DMZ)</td><td>암호화 저장</td></tr>
<tr><td>내부망에 저장</td><td>암호화 저장 또는 다음 항목에 따라 암호화 적용 여부,
적용범위를 정하여 시행 가능

1.개인정보 영향평가 대상이 되는 공공기관의 경우,
그 개인정보 영향평가의 결과

2. 암호화 미적용 시 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터,
모바일 기기에 저장 시</td><td colspan="3">비밀번호, 바이오정보, 고유식별 정보</td><td>암호화 저장

1. 비밀번호는 일방향 암호화 저장
2. 상용 암호화 소프트웨어 또는 안전한 알고리즘 암호화</td></tr>
</table>

4. 관련규정 및 조치기준

개인정보 암호화 대상 및 방법

암호화 필요 대상

고유식별정보
비밀번호
바이오정보

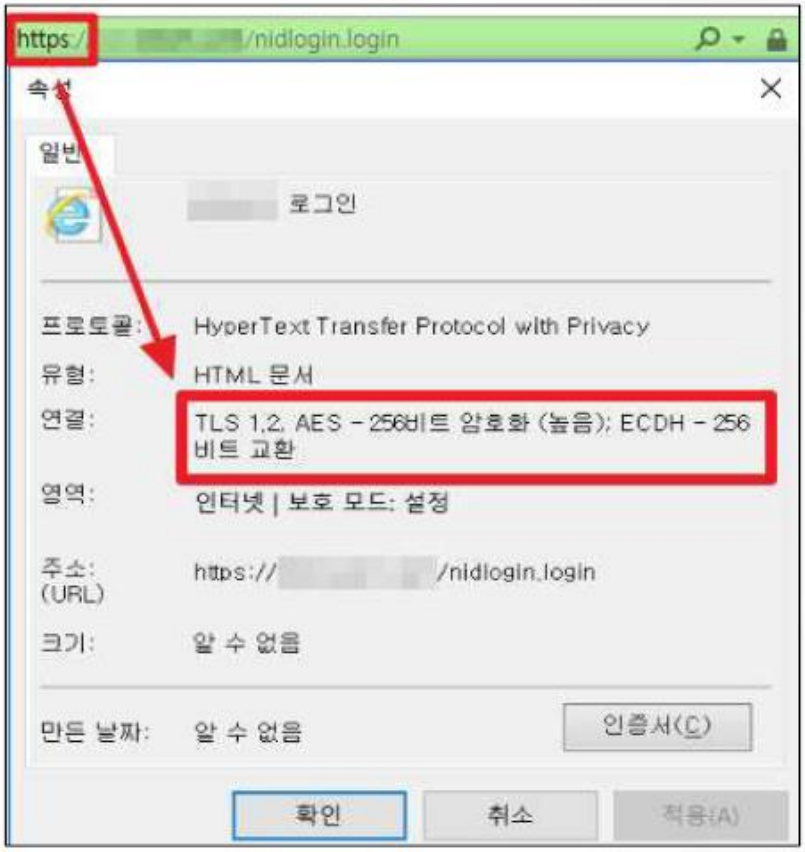
보안강도	해쉬 함수	안정성
80 비트 미만	MD5, SHA-1	권고하지 않음
80 비트	HAS-160	
112 비트	SHA-224	2013년까지 권고함
128 비트	SHA-256	2013년 이후에도 가능
192 비트	SHA-384	
256 비트	SHA-512	

① 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행

② 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장

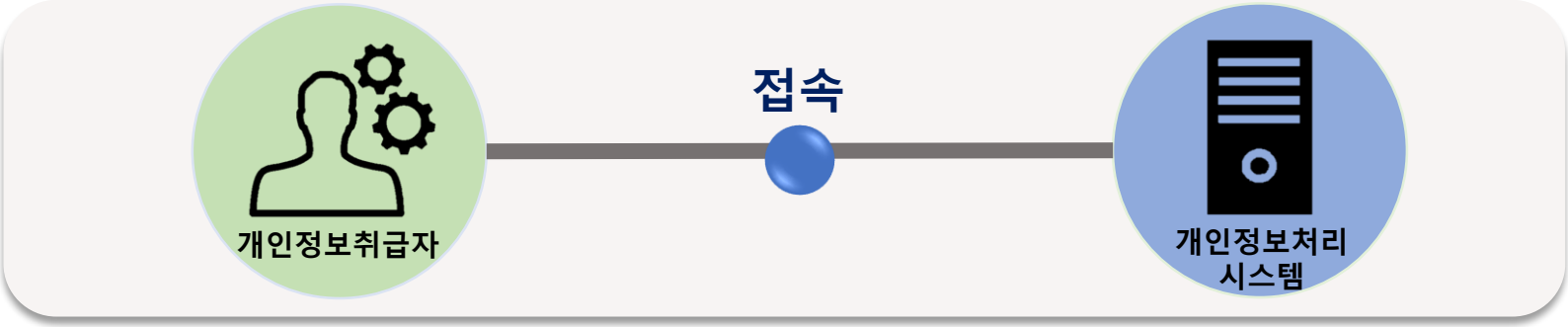
4. 관련규정 및 조치기준

개인정보 암호화(제7조) 위반사례

법령	개선조치
제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.	

4. 관련규정 및 조치기준

접속기록의 보관 및 점검(제8조)



① 개인정보 취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 안전하게 보관・관리(5만명이상 2년)

② 개인정보처리시스템의 접속기록 등을 월1회 이상 점검

필수 기록 항목
- 계정 : 개인정보취급자 계정
- 날짜 및 시간 : 접속 일시
- 접속자 IP 주소 : 접속지 정보
- 정보주체 정보: 정보주체자의 식별정보
- 수행 업무 : 열람, 수정, 삭제, 인쇄 입력 등

별도 물리적인 저장 장치에 보관하고 정기적인 백업 수행
- 접속기록 위・변조 방지를 위해 CD-ROM 같은 덮어쓰기 방지 매체 사용
- 수정 가능한 매체 백업 시, 위・변조 여부를 확인할 수 있는 정보(HMAC or 전자서명 등)를 별도 장비에 보관・관리

4. 관련규정 및 조치기준

접속기록의 보관 및 점검(제8조) 위반사례

법령	위반사례
제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. (5만명 이상의 정보주체 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 시스템의 경우 2년 이상) 제2조(정의) 19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다. (자료설명 : 정보주체, 수행업무에 대한 접속 기록을 보관하고 있지 않음)	

관리자 아이디 체크

*입력/수정 DATA 설명
N -> 변경안함 , Y -> 변경
좌측 데이터부터 이름 | 이메일 | 생년월일 | 주소 | 전화번호 | 휴대폰 ex) Y|N|Y|N|Y|N

아이디	이벤트	IP	시간	사용자ID	입력/수정 DATA
admin	login	192.	2016-11-21 13:20:10.0		
null	logout		2016-11-21 13:19:47.0		
admin	login	192.	2016-11-21 13:08:14.0		
qwerty	login	192.	2016-11-21 12:59:22.0		
qwerty	login	192.	2016-11-21 11:54:17.0		
qwerty	login	192.	2016-11-21 11:08:41.0		
qwerty	login	192.	2016-11-21 11:03:47.0		
qwerty	login	192.	2016-11-21 11:01:29.0		
admin	login	192.	2016-11-21 10:39:04.0		
qwerty	login	192.	2016-11-21 10:28:22.0		
qwerty	login	192.	2016-11-21 10:27:28.0		
qwerty	login	192.	2016-11-21 10:21:25.0		
qwerty	login	192.	2016-11-21 10:21:03.0		
qwerty	login	192.	2016-11-21 10:17:48.0		
qwerty	login	192.	2016-11-21 10:01:16.0		
qwerty	login	192.	2016-11-21 09:59:19.0		
qwerty	login	192.	2016-11-21 09:58:19.0		
qwerty	login	192.	2016-11-21 09:46:19.0		
admin2	logout	125.1	2016-11-21 09:44:10.0		
admin2	login	125.1	2016-11-21 09:43:32.0		

1 2 3 4 5 6 7 8 9 10 [Next] 957

4. 관련규정 및 조치기준

악성프로그램 방지(제9조)

악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영해야 함

① 보안 프로그램은 항상 최신의 상태로 유지

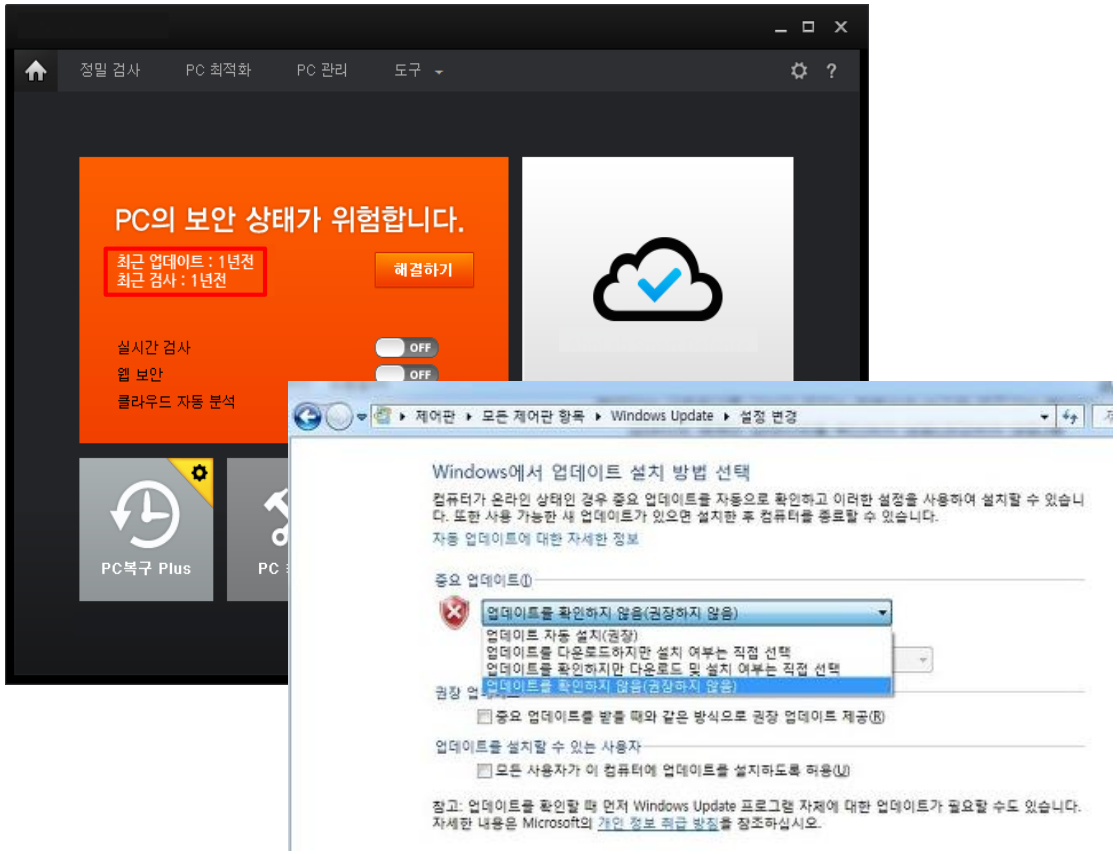
- 자동 업데이트 기능 사용
- 일 1회 이상 업데이트 실시

② 악성프로그램 관련 경보 발령 또는 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트 실시

③ 발견된 악성 프로그램 등에 대해 삭제 등 대응 조치

4. 관련규정 및 조치기준

악성프로그램 방지(제9조) 위반사례

법령	위반사례
제9조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다. 1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시 3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치 (자료설명 : 백신 소프트웨어 업데이트 미 실시)	

4. 관련규정 및 조치기준

관리용 단말기 안전조치(제10조)

관리용 단말기

개인정보처리시스템의 관리, 운영,
개발, 보안 등의 목적으로
개인정보처리시스템에 직접 접속하는 단말기

① 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

② 본래 목적 외로 사용되지 않도록 조치

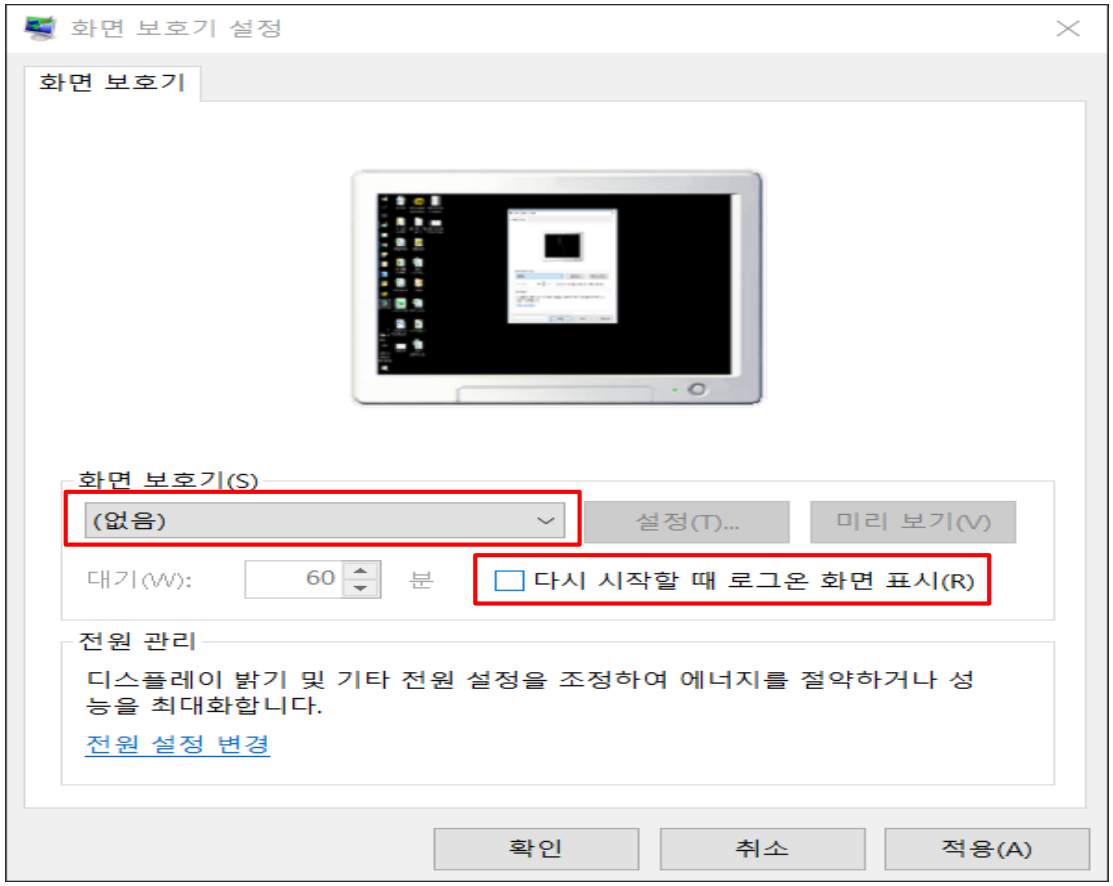
③ 악성프로그램 감염 방지 등을 위한 보안 조치 적용

고려사항

- 관리용 단말기의 종류에 따른 특성, 중요도
- 개인정보처리시스템에 **접속하는 빈도 및 수행업무**
- 관리용 단말기를 통한 개인정보의 **유출 가능성** 및 개인정보처리시스템에 악성코드 전파 등

4. 관련규정 및 조치기준

관리용 단말기 안전조치(제10조) 위반사례

법령	위반사례
제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다. 1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 2. 본래 목적 외로 사용되지 않도록 조치 3. 악성프로그램 감염 방지 등을 위한 보안조치 적용 제2조(정의) 20. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다. (자료설명 : 관리용 단말기에 화면 보호기 설정이 미흡하여, 비 인가자 접근이 가능함)	

4. 관련규정 및 조치기준

물리적 안전조치(제11조)

① 개인정보 보관을 위한 물리적 보관 장소(전산실, 자료보관실 등)는 출입 통제 절차를 수립. 운영

② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관

③ 개인정보가 포함된 보조저장매체의 반출.입 통제를 위한 보안대책을 마련

- 다만, 별도의 개인정보처리시스템 없이 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우는 예외

4. 관련규정 및 조치기준

물리적 안전조치(제11조)

법령	위반사례
제11조(물리적 안전조치) ② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금 장치가 있는 안전한 장소에 보관하여야 한다. (자료설명 : 개인정보가 포함된 서류, 보조저장 매체 등을 책상위에 보관하고 있음)	

4. 관련규정 및 조치기준

재해 • 재난 대비 안전조치(제12조)

화재, 홍수, 단전 등의 재해. 재난 발생 시

① 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검

② 개인정보처리시스템 백업 및 복구를 위한 계획 마련

4. 관련규정 및 조치기준

재해 • 재난 대비 안전조치(제12조) 위반사례

법령	위반사례
제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보 처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다. ② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다. ③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다. (자료설명 : 재해재난 대비 위기대응 절차 미 수립)	**개정 전** 없음 **개정 후(2016.08.31 시행)** ① 재해재난 대비 위기대응 매뉴얼 등 대응절차 수립 및 정기 점검 ② 재해재난 대비 개인정보처리시스템 백업 및 복구를 위한 계획 수립 ③ 유형 1,2 : 제1항, 제2항 예외 유형3(강화) 10만 명 이상의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 이상의 개인정보를 보유한 중소기업, 단체

4. 관련규정 및 조치기준

개인정보 파기

① 개인정보 파기 조치

- 완전파괴 (소각·파쇄 등)
- 전용 소자장비 이용하여 삭제
- 데이터가 복원되지 않게 초기화 또는 덮어쓰기

② 1항의 방법이 어려울 경우 일부 파기 조치

전자적 파일 형태인 경우

개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우

해당 부분을 마스킹, 천공 등으로 삭제

참고자료

개인정보보호 생활규칙 등 참고사항

개인정보보호 생활규칙 등 참고사항

개인정보 오남용 피해 방지 10계명

※ 개인정보를 "똑~ 소리나게 지켜내기" 위해서 인터넷 사용시 또는 생활속에서 실천해야 함

❖ 개인정보 침해신고 적극 활용하기

개인정보가 유출된 경우 즉시 개인정보 침해신고하기

☞ privacy.kisa.or.kr

❖ 개인정보처리방침 및 이용약관 꼼꼼히 살피기

개인정보 처리자는 개인정보 취급 관련 내용을 개인정보처리방침에 포함하여 공개해야함

❖ 비밀번호는 문자와 숫자로 8자리 이상

쉽게 추측이 불가능하고 해킹을 당하더라고 패스워드를 알아내는데 많은 시간이 요구되도록 영문/숫자 등을 조합하여 8자리 이상으로 설정

❖ 비밀번호는 주기적으로 변경하기

자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 주기적으로 비밀번호 변경

❖ 회원가입은 주민번호 대신 I-PIN 사용

가급적 안정성이 높은 주민번호 대체수단(아이핀)으로 회원가입하고, 불필요한 개인정보의 입력은 하지 않기

❖ 명의도용확인 서비스 이용하여 가입정보 확인

타인이 자신의 명의로 신규회원가입 시 즉각 차단하고, 이를 통지받을 수 있도록 명의도용 확인서비스를 이용

❖ 개인정보는 친구에게도 알려주지 않기

자신의 아이디/비밀번호/주민번호 등이 공개되지 않도록 주의하여 관리하고 친구나 다른 사람에게 알려주지 않기

❖ P2P공유폴더에 개인정보 저장하지 않기

인터넷에 올리는 데이터에 개인정보가 포함되지 않도록 하며, P2P로 제공하는 공유폴더에 개인정보 파일이 저장되지 않도록 하기

❖ 금융거래는 PC방에서 이용하지 않기

금융거래 시 신용카드번호 등 금융정보를 저장할 경우 암호화하고 PC방 등 개방 환경을 이용하지 않기

❖ 출처가 불명확한 자료는 다운로드 금지

회원가입을 하거나 개인정보를 제공할 때에는 개인정보처리방침 및 약관을 꼼꼼히 살피고 출처불명의 자료는 다운로드에 주의하기

개인정보보호 생활규칙 등 참고사항

1 공공기관장, CPO 등은 개인정보보호 마인드 제고가 필요합니다!

- 개인정보보호 업무가 내부 사업 중요도에서 후순위로 밀리는 사례 다수 발견
- 보직자의 개인정보에 대한 중요성을 인식하고 많은 관심과 적극적인 지원 필요

2 안전한 개인정보 보관·관리를 위해 적극적인 투자를 해주세요!

- 정보보호시스템* 등 투자 부족으로 '개인정보 안전성 확보조치 기준' 위반사항 다수 발견
  * 침입차단시스템, 침입탐지시스템, 침입방지시스템, 웹방화벽, DB접근제어시스템, DB암호화솔루션 등
- 공통시스템(예:새올행정)에 비해 자체 개발·도입 시스템이 취약
- 특히 노후화된 시스템의 법규 준수여부를 체크 필요
- 적정 예산 확보를 통한 지속적인 투자 당부

개인정보보호 생활규칙 등 참고사항

3 개인정보보호 전담인력을 배치·교육하고 전문성을 높여주세요!

- 전담인력이 없거나 전담인력의 잦은 교체로 업무 연속성 미흡 사례 빈번
- 개인정보파일 현황 파악 미흡, 내부관리계획 등 규정 정비 미흡 등 발견
- 보안 전문교육 등을 통해 개인정보보호 및 정보보호 인력의 안정적인 운영 필요

4 개인정보 유출사고의 주요 원인인 해킹방어에 힘써주세요!

- 사용 중인 OS 등 소프트웨어에 대한 최신 보안 업데이트 상시 적용(랜섬웨어)
- 홈페이지 개발 시 시큐어코딩 사용, 개발된 홈페이지의 경우 주기적인 웹취약점 분석
- 방화벽 등 보안장비의 보안정책을 주기적으로 점검 및 최신 이슈사항 반영
- 송신자가 명확하지 않은 메일 열람 금지, 블로그 등에서 받은 프로그램 실행 금지

개인정보보호 생활규칙 등 참고사항

5 개인정보가 유출되었을 때는 정보주체에게 알려주세요!

- 유출된 정보주체 개개인에게 지체없이(5일이내) 통지(유출 항목/시점/경위, 대응방안)
- 1만명 이상 유출된 경우에는 유출통지 결과를 행안부/KISA에 신고하고 홈페이지에 공지
- 피해 최소화를 위한 대책 마련 및 필요한 조치 실시(유출된 개인정보의 삭제 등)

6 법령 및 고시 재·개정 사항을 지속적으로 모니터링 해주세요!

- '16.9. 시행된 '일정시간 미작동시 로그아웃', '비밀번호 오류 계정잠금' 등 미조치 다수
- 언론 등을 통해 법령 및 고시 재·개정 사항을 파악하고 법적 요구사항을 반영

개인정보보호 생활규칙 등 참고사항

점검도구 신청 대상

- 소상공인(상시종업원 5인 미만)
- 중소사업자(상시종업원 50인 미만 또는 중소기업확인서 등 발급받은 사업자)
- 수익사업을 하지 않는 비영리단체(상시종업원 수 상관없음)

개인정보보호 생활규칙 등 참고사항

- ① 개인정보보호 종합포털(www.privacy.go.kr)에서 신청

  ※ 신청 경로 : 종합포털 →사업자→개인정보보호 기술지원→업무용 PC 보호조치 점검도구 신청

- ② 안내메일 확인
- ③ 증빙서류 등 제출(이메일)
- ④ 이메일에 점검도구 프로그램 첨부하여 발송

  ※ 증빙서류 접수 후 점검도구 프로그램 발송까지 약 5일 정도 소요

개인정보보호 생활규칙 등 참고사항

업무용PC 점검도구 신청 대상

소상공인·중소사업자 등을 대상으로 업무용 PC에 대한 개인정보 보호조치를 자율적으로 수행할 수 있도록 프로그램 무료 제공

업무용 PC 개인정보 보호조치 점검도구 주요 기능	
개인정보 암호화 점검	업무용 PC 내 개인정보 파일에 포함된 주민등록번호 등 고유식별정보 등 암호화 대상 정보에 대한 암호화 여부 점검 및 조치방법 안내
비밀번호 관리	비밀번호 작성규칙의 적절성, 비밀번호 유효기간 확인 등 점검 및 조치방법 안내
접근통제 시스템 설치·운영 점검	방화벽 설정, P2P·공유설정 여부에 대한 점검 및 조치방법 안내
보안프로그램 설치·운영 점검	백신 등 보안프로그램의 설치 및 업데이트 여부 등 점검 및 조치방법 안내

[참고]

e 프라이버시 클린서비스 소개

e프라이버시 클린서비스(eprivacy.go.kr) - 소개

- **(본인확인 내역조회)** 인터넷에서 회원가입, 연령확인(성인인증), 실명인증 등을 위해 실시된 주민번호 및 아이핀, 휴대폰, 신용카드 등의 주민번호 대체수단을 통한 본인확인 내역 통합 조회 제공
- **(회원 탈퇴 지원)** 명의도용이 의심되거나 아이디·비밀번호 등을 알지 못해 회원탈퇴에 어려움이 있는 경우, 더 이상 이용을 원하지 않는 불필요한 웹사이트에 대한 회원탈퇴 처리 대행

e프라이버시 클린서비스 - 추진배경과 이용절차

추진근거(1)

개인정보보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. **개인정보의 처리에 관한 정보를 제공받을 권리**
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. **개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람**을 요구할 권리
4. **개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리**
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

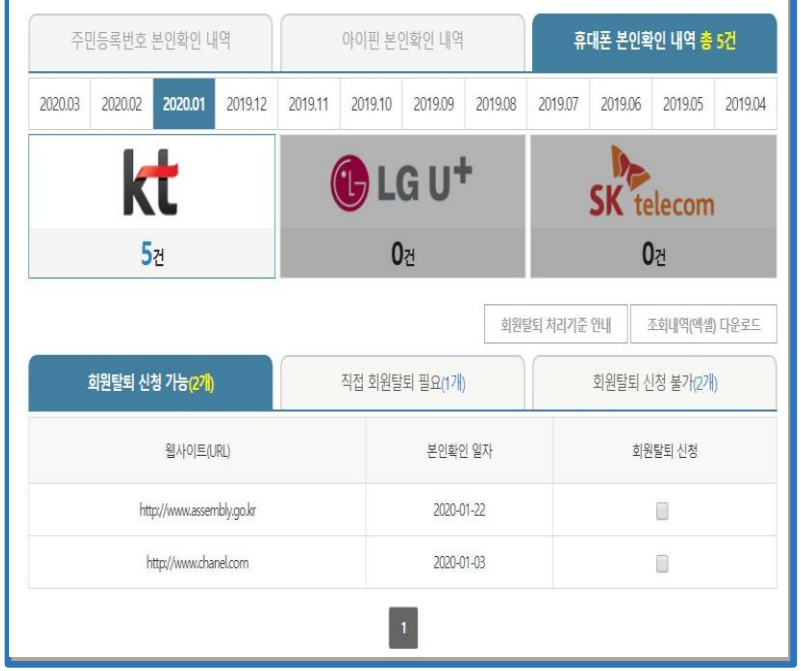
e프라이버시 클린서비스 – 본인확인 내역조회

추진근거(2)

개인정보보호법 제37조(개인정보의 처리정지 등)

① **정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다.**
이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.

본인확인 내역조회 화면



본인확인 내역조회 종류

구 분	주민번호	휴대폰	아이핀
제공기간	5년	1년	1년(공공) 5년(민간)
정보제공	신용평가3사	이통3사	신용평가3사 & KLID

✓신용평가사(3): SCI평가정보, NICE평가정보, 코리아크레딧뷰로(KCB)

✓이동통신사(3) : SK, KT, LGU+(알뜰폰 포함)

e프라이버시 클린서비스 – 본인확인 내역조회

추진근거(3)

제38조(권리행사의 방법 및 절차) ① 정보주체는 **제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.**

회원탈퇴 신청

회원탈퇴 유형

회원탈퇴 신청가능	직접 회원탈퇴	회원탈퇴 신청불가
회원제 사이트	간편 회원가입	비회원제 사이트
	온-오프라인 연계 회원	인트라넷 (비공개)
	서비스 일시중지	접속불가
	회원탈퇴 일시보류	소재불명
	웹사이트 운영자 비협조	해외사이트
		부정확한 URL

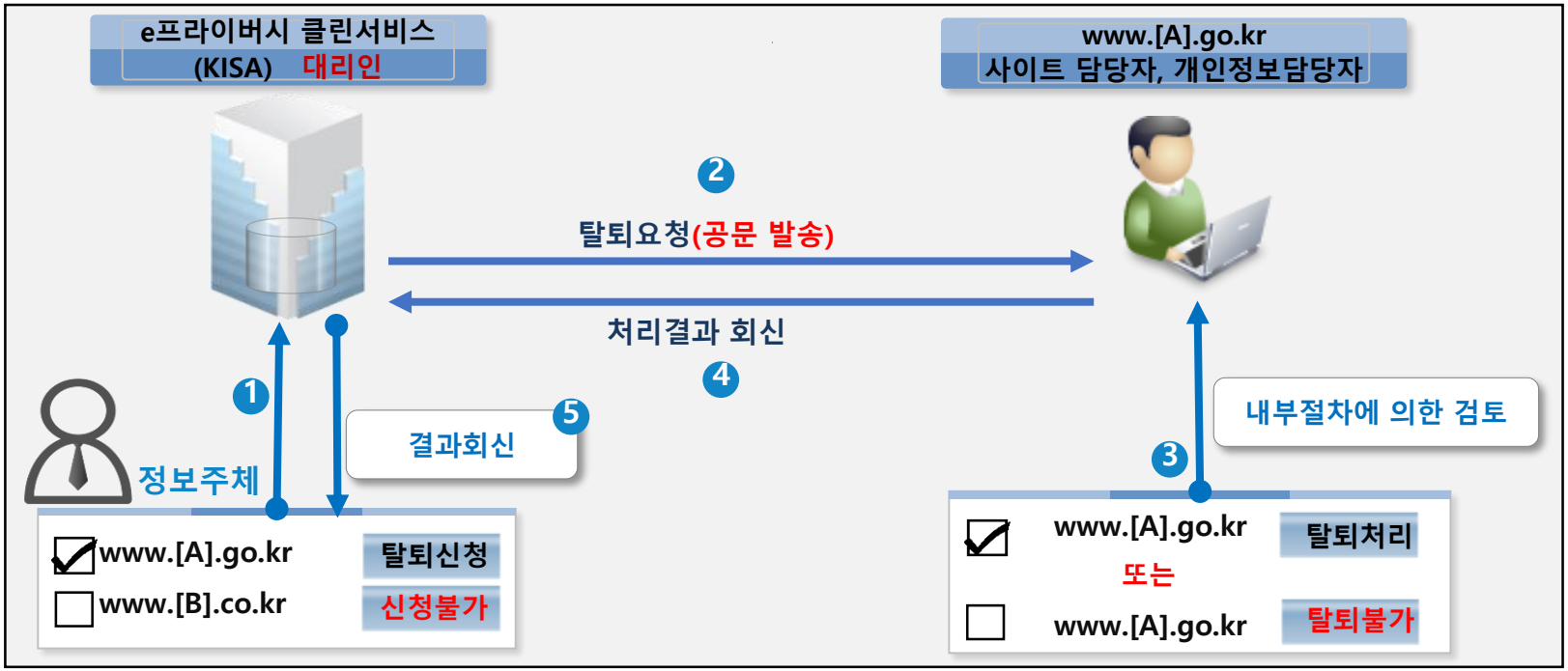
e프라이버시 클린서비스- 회원탈퇴 절차(1/2)

절차

☞ 미회신 기관은 법적 제재 대상으로 분류됨

공문발송 → 회원가입 여부 확인 → 회원탈퇴 조치 → 처리결과 통보서 작성 → 처리결과 통보

- 공문발송: KISA — 회원가입 여부 확인 및 회원탈퇴 요청
- 회원가입 여부 확인: 개인정보처리 시스템 — 회원탈퇴 신청내역 참고
- 회원탈퇴 조치:
  1. [회원이 아닌 경우] 회원가입 여부 사실 확인
  2. [회원인 경우] 회원탈퇴 필요조치 (처리정지, 파기 등)
- 처리결과 통보서 작성: [처리결과 통보서] 처리결과 분류표 참고
- 처리결과 통보: [공문 또는 이메일 발송] 처리결과 통보서 첨부



e프라이버시 클린서비스- 회원탈퇴 절차(2/2)

추진근거

☞ 정보주체의 권리 보장(개인정보처리자 의무사항)

개인정보보호법 시행령 제44조(개인정보의 처리정지 등)

② 개인정보처리자는 개인정보 처리정지 요구를 받은 날부터 10일 이내에 해당 개인정보의 처리정지 조치를 한 경우에는 그 조치를 한 사실을, 처리정지 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 행정안전부령으로 정하는 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.

"법률 근거 확인 후 처리결과 10일 이내 정보주체에게 통지"

이를 위반할 경우 2년 이하 징역 및 3천만원 과태료 부과(법73조, 법75조)

e프라이버시 클린서비스 – 회원탈퇴 처리 유형(1/2)

- **회원탈퇴 처리 요청에 대한 사업자 회신**

구분	내역	사유
회원탈퇴 처리 가능	회원탈퇴 완료	KISA의 요청에 따라 회원탈퇴 조치 완료
회원탈퇴 처리 불가	온·오프라인 연계회원	온라인 회원탈퇴 시 오프라인 회원 자격도 상실되는 경우
	복수 아이디 보유	민원인이 해당 웹사이트에서 2개 이상 아이디를 발급·보유하고 있어, 어떤 아이디를 회원탈퇴 처리해야 하는지 불분명한 상태
	인트라넷	서비스 이용 대상이 특정 기업(기관)의 임직원·관계자 등으로 제한되고, 접속 권한 부여/상실도 해당 기업(기관)에서 직접 관리하는 경우
	회원탈퇴 시 불이익 발생	하나의 아이디로 복수의 웹사이트가 연동되는 통합 회원제 사이트로, 하나의 웹사이트 회원탈퇴 시 타 웹사이트 이용에 영향을 받는 경우
		탈퇴 시 이메일 및 첨부자료, 각종 게시물 등의 자료 손실이 우려되는 경우
		아이템, 사이버머니, 캐시, 쿠폰, 포인트, 마일리지, 적립금 등이 남아 있거나 요금 등이 미납 상태인 경우(소멸, 정산 문제 발생)
		봉사확인서, 기부명세서, 교육수료증, 장기기증, 개인회생 및 파산, 민형사상 소송기록 등의 자료가 포함된 경우
	간편 회원가입	이메일, 휴대전화번호 등 단일정보만으로 가입되어 민원인 본인을 명확히 확인할 수 없는 경우(타인에 의한 탈퇴신청 방지)
	회원탈퇴 일시보류	채용·모집 또는 법령에서 정한 사유 등을 목적으로 가입을 받은 후 회원정보를 바탕으로 일정기간 업무 진행 중(해당 업무 종료 후 탈퇴 가능)

e프라이버시 클린서비스 – 회원탈퇴 처리 유형(2/2)

- **회원탈퇴 처리 요청에 대한 사업자 회신**

구분	내역	내용
회원탈퇴 의사 철회	회원탈퇴 신청 취소 (민원인 취소)	e프라이버시 클린서비스에 회원탈퇴 신청 후, 민원인이 직접 웹사이트 운영자에게 연락하여 회원탈퇴 신청을 취소한 경우
	웹사이트 지속 사용	회원탈퇴 신청한 이후에도 민원인이 해당 웹사이트에 접속·이용하는 것으로 확인되어, 웹사이트를 지속 이용할 의향이 있는 것으로 간주
	회원탈퇴 신청 취소 (웹사이트 확인에 의한 취소)	E프라이버시 클린서비스에 회원탈퇴 신청 후, 웹사이트 운영자가 직접 민원인에게 연락하여 문의한 결과 회원탈퇴 신청취소 의사를 밝힌 경우
기타	비회원	신청인이 해당 웹사이트에 회원 가입된 이력이 없거나 이미 회원탈퇴 처리가 되어 있는 경우
	비회원(이용정지)	민원인이 해당 웹사이트의 이용약관 등을 위반 (상업적 홍보물, 음란물 게시, 욕설, 비방 등)하여 이용 정지된 상태
	민원인 식별 불가	KISA에서 송부한 개인정보(ID, 이름, 생년월일, 이메일, 전화번호)로는 민원인 확인(식별) 불가
	휴면계정	민원인이 탈퇴 요청한 계정이 휴면계정으로 전환된 경우

회원탈퇴 요청 및 결과 회신(공문 예시)

- **회원탈퇴 처리 요청 공문(KISA 발송)**

KISA 한국인터넷진흥원

수신자 해당 웹사이트 운영자(개인정보보호책임자)
(경유)
제 목 민원인의 웹사이트 회원가입 여부 확인 및 회원탈퇴 처리 요청

1. 한국인터넷진흥원 개인정보침해신고센터는 관련 법령*에 따라 정보주체의 개인정보에 관한 권리 또는 이익 침해 사실의 신고 접수·상담 및 처리 등에 관한 업무를 수행하고 있습니다.
   * 개인정보보호법 제62조(침해 사실의 신고 등) 및 동법 시행령 제69조(침해사실의 신고 등), 정보통신망법 시행령 제66조(개인정보침해신고센터의 운영) 등

2. 위의 일환으로 우리원은 행정안전부와 공동으로 정보주체의 알 권리 보장 및 개인정보자기결정권 강화를 위해 e프라이버시 클린서비스(www.eprivacy.go.kr)*를 제공하고 있습니다.
   * 주민등록번호 및 주민등록번호 대체수단(아이핀, 휴대폰)을 통한 본인확인(인증) 내역 통합 조회 및 명의도용이 의심되거나 원치 않는 웹사이트에 대한 회원탈퇴 지원서비스 제공

3. e프라이버시 클린서비스를 통해 귀 기관(기업)에서 운영하고 있는 웹사이트에 대한 회원탈퇴 요구 민원이 접수되었으니, 아래의 내용을 확인하시어 민원인의 고충이 해소될 수 있도록 적극 협조해주시기 바랍니다.

   가. 근거법령 : 「개인정보보호법」 제4조(정보주체의 권리), 제37조(개인정보의 처리정지 등) 및 제38조(권리행사의 방법 및 절차), 「정보통신망법」 제30조(이용자의 권리 등) 등
   나. 요청내용 : 민원인(별첨자료 참고)의 회원가입 여부 확인 및 회원탈퇴 조치(개인정보 처리정지, 파기 등)
   ※ 민원인의 신원은 e프라이버시 클린서비스의 본인확인 및 이용자 정보 입력 절차를 통해 확인함
   다. 결과통보 : 「회원탈퇴 처리결과 통보서(붙임2)」 작성 후 회신
   라. 문 의 처 : 02-408-7843
   마. 유의사항 : 정당한 사유 없이 민원인의 회원탈퇴 처리 요청에 응하지 아니하거나 허위로 처리결과를 회신하는 경우, 「개인정보보호법」 제75조제2항제10호 및 「정보통신망법」 제76조제1항제5호 등에 따라 처벌받을 수 있음

붙임 1. 회원탈퇴 처리 안내문 1부
2. 회원탈퇴 처리결과 통보서 1부. 끝.

한국인터넷진흥원장

- **회원탈퇴 처리결과 회신(웹사이트 담당자)**

저작권 존중과 나눔, 모두가 행복해집니다.

한국

수 신 한국인터넷진흥원장
(경유) 개인정보대응센터
제 목 민원인의 웹사이트 회원가입 여부 확인 및 회원탈퇴 처리 요청에 대한 회신

1. 귀 기관의 무궁한 발전을 기원합니다.

2. 개인정보대응센터-2018-5355(2018.08.09.) 관련입니다.
3. 위 관련으로 귀 기관에서 웹사이트 회원가입 여부 확인 및 회원탈퇴 처리 요청에 대해 회신합니다.
   가. 요청사항 : 웹사이트( ) 회원 가입 여부 확인 및 회원탈퇴
   나. 처리결과 : 첨부파일
   다. 처리방식 : 웹사이트 회원 가입 여부 확인 후 탈퇴 의사 본인 확인
   라. 담 당 자 : 한국 기반팀 이 (☎055- -02)
붙 임 한국 웹사이트 회원탈퇴 처리결과. 끝.

홈페이지 개인정보 노출예방

질/의/응/답

KISA 한국인터넷진흥원

Internet On, Security In!

Thank you

개인정보보호 종합포털	www.privacy.go.kr
e프라이버시 클린서비스	www.eprivacy.go.kr
개인정보침해신고센터	(국번없이) 118
	(홈페이지) privacy.kisa.or.kr