홈페이지 개인정보
노출방지 안내서

2016.06

행정자치부 한국인터넷진흥원

제 · 개정 이력

본 "홈페이지 개인정보 노출방지 안내서" 는 '08년 2월 제정 이후 5차 개정판입니다.

구분	일자	비고
제정	2008.02	
1차 개정	2009.02	
2차 개정	2011.05	
3차 개정	2012.08	
4차 개정	2014.12	
5차 개정	2016.06	

· 본 안내서는 「개인정보 보호법」 등 관계법령의 규정을 토대로,

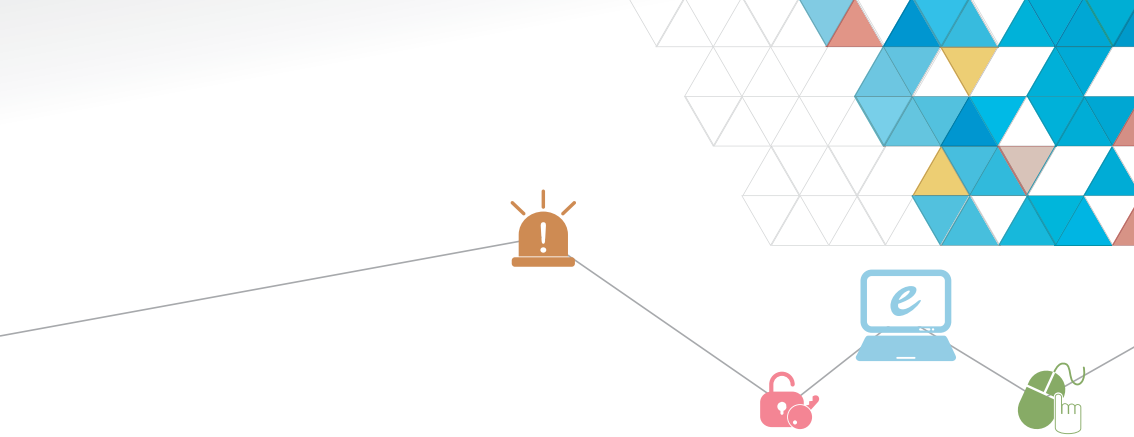
  – 개인정보 담당자, 홈페이지 담당자 및 홈페이지 개발자를 대상으로 인터넷에 노출된 개인정보의 오남용을 예방하기 위하여 개인정보 노출 원인별 구체적인 사례 및 조치방법에 대한 올바른 이해를 돕기 위한 목적으로 발간되었습니다.

  – 다만, 다른 사람이 게시하거나 공개한 개인정보를 삭제할 때에는 임의 삭제 조치가 타인의 재산권 침해 등의 우려가 있는지 여부를 반드시 확인 후 조치해야 합니다.

· 본 안내서에서 제공하는 조치방법 및 처리절차 예시 등은 각 기관의 고유한 특성 및 환경에 맞게 적용 하시면 됩니다.

※ 본 안내서는 개인정보보호 종합포털 홈페이지 [www.privacy.go.kr - 자료마당 - 지침자료]와 개인정보보호 포털 [www.i-privacy.kr - 자료실 - 안내서 및 해설서]에 게시될 예정입니다.

CONTENTS



Ⅰ 개요

1. 개인정보란?
2. 개인정보 노출이란?
3. 개인정보 노출 시 어떤 위험이 있나요?

Ⅰ 개요

1. 개인정보란?

개인정보란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말합니다. 또한, 해당 정보만으로는 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 경우, 개인정보에 포함됩니다(개인정보 보호법 제2조 제1호). 즉, 하나의 정보 혹은 두 개 이상의 정보들이 모여서 개인을 식별할 수 있다면 개인정보라고 할 수 있습니다.

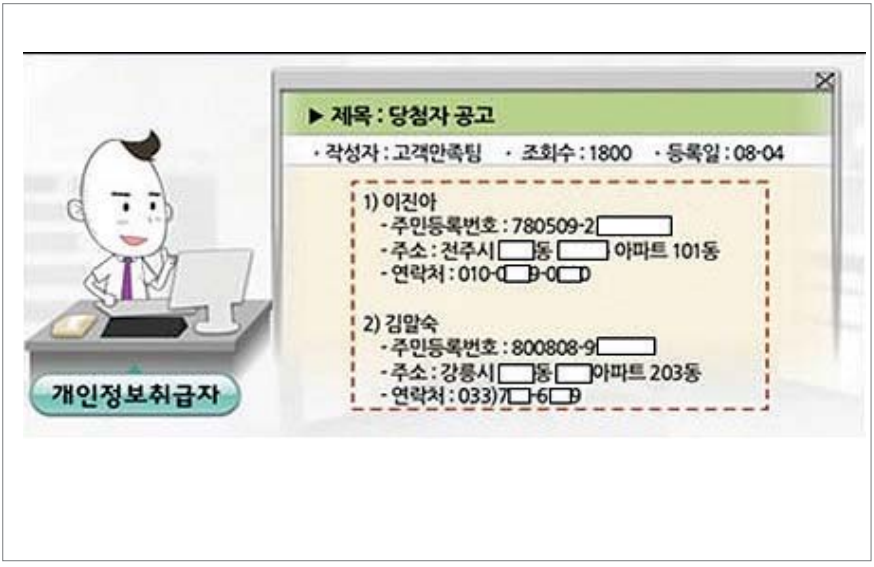
개인정보의 범위는 과거에는 이름, 주민등록번호, 생년월일, 주소 등의 단순한 신분정보를 의미하였으나 오늘날에는 개인의 위치정보, 바이오정보를 비롯한 개인의 기호, 성향, 신념, 사상까지 포함될 정도로 매우 광범위해졌습니다. 이러한 개인정보가 노출되어 악용될 경우 막대한 경제적 · 정신적 피해가 발생할 수 있으므로 홈페이지를 통해 노출되지 않도록 특별히 주의해서 관리해야 합니다.

[표 1] 개인정보의 유형(예)

구분	유형	구분	유형
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적	가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 기술 자격증 및 전문 면허증, 학교성적, 동아리활동, 상벌사항, 이수한 훈련 프로그램,	병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등	소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타수익 정보	보험(건강, 생명 등) 가입현황, 병가, 휴가, 회사의 판공비, 투자프로그램, 퇴직프로그램	신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 출석기록, 상벌기록, 성격테스트 결과 직무태도	법적정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보	조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화내용, 로그파일(log file), 쿠키(cookies)	위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등	습관 및 취미정보	음주량, 선호하는 스포츠 및 오락, 흡연, 여가활동, 비디오 대여기록, 도박성향

2. 개인정보 노출이란?

개인정보 노출이란 홈페이지를 이용하는 자(이하 홈페이지 이용자)가 해킹 등 특별한 방법을 사용하지 않고, 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷상에서 관련 정보가 방치되어 있는 상태를 말합니다. 노출되는 주요 개인정보는 주민등록번호, 여권번호, 전화번호, 휴대폰번호 등 다양하게 나타날 수 있으며, 이러한 개인정보는 손쉽게 노출이 가능하므로 항상 주의가 필요합니다.



[그림 1] 개인정보 노출 예시

3. 개인정보 노출 시 어떤 위험이 있나요?

개인정보가 노출되면 사생활 침해와 같은 직접적인 피해가 발생할 수 있습니다. 그리고 노출된 개인정보를 신속히 삭제하지 않을 경우, 외부 검색엔진에 의해 노출된 정보가 확산되거나 제3자에게 개인정보가 수집되어 개인정보의 통제권을 상실하게 되므로 2차 피해가 발생할 수 있습니다.

개인의 경우에는 명의도용, 보이스피싱 등에 의한 금전적 손해 및 각종 범죄에 악용될 우려가 있으며, 기업의 경우에는 이미지 실추, 소비자 단체 등의 불매운동, 다수 피해자에 대한 손해배상 등으로 기업경영에 큰 타격을 입을 수 있습니다.

개인정보 노출을 예방하는 최선의 방법은 개인정보 수집을 최소화하는 것입니다. 민감정보와 고유식별정보는 법령에서 규정하고 있거나 정보주체로부터 별도의 동의를 받은 경우에만 수집이 가능합니다. 특히, 주민등록번호는 법령으로 정하거나 급박한 생명 · 신체 · 재산상 이익을 위하여 명백히 필요한 경우만 수집이 가능하고, 정보주체의 동의를 받더라도 수집 · 이용을 할 수 없도록 법령에 명시되어 있습니다.

또한, 보유하고 있던 개인정보가 불필요(보유기간의 경과, 개인정보의 처리 목적 달성 등)하게 되었을 때에는 해당 개인정보를 지체 없이 파기해야 합니다.

개인정보 보호법 상 용어정의

* 민감정보 : 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보(제23조)
  ※ 정보통신망법 적용 사업자는 정보통신망법 제23조 참조/적용/반영
* 고유식별정보 : 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호(시행령 제19조)

※ 2017.03.30.부터 주민등록번호는 법률, 시행령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙에 근거가 있어야 처리가능 함 (개인정보 보호법 제24조의2 제①항)

Ⅱ 개인정보 노출 원인별 사례분석

1. 홈페이지 설계 및 관리 미흡으로 인한 노출
2. 첨부파일에 의한 노출
3. 게시글에 의한 노출

Ⅱ 개인정보 노출 원인별 사례분석

홈페이지를 통해 개인정보가 노출되는 주요 원인은 홈페이지 설계 및 관리 미흡, 첨부파일 노출, 게시글 노출이 대부분입니다. 홈페이지 설계 및 관리 미흡에 의한 노출은 시스템 전반에 영향을 미치기 때문에 대량노출로 이어질 가능성이 높으며, 기술적인 조치가 필요한 부분이므로 개발 또는 운영 담당자와 같이 해결해야 합니다.

첨부파일에 의한 노출은 홈페이지 이용자가 첨부파일을 다운로드하여 개인 PC에 저장하는 경우가 많아, 홈페이지 서버에서 해당 첨부파일을 삭제하더라도 이미 외부로 노출된 파일은 삭제할 수 없기 때문에 개인정보가 유출될 위험성이 높습니다.

게시글에 의한 노출은 개인정보 취급자가 공지사항 작성이나 민원 처리 시 부주의하여 개인정보가 노출되거나, 또는 홈페이지 이용자가 민원을 작성하거나 예약확인 요청 등을 위해 자신의 개인정보를 공개하여 개인정보가 노출되는 경우에 발생할 수 있습니다.

이렇듯 개인정보 노출을 발생시키는 주체에 따라 개인정보 취급자가 작성한 첨부파일 등을 통해 개인정보 노출이 발생하는 경우에는 개인정보 취급자 부주의, 홈페이지 이용자가 작성한 게시글 등을 통해 개인정보 노출이 발생하는 경우에는 홈페이지 이용자 부주의로 구분할 수 있습니다.

또한 홈페이지 설계 및 구현이 잘못된 경우 또는 홈페이지의 서버의 설정이 잘못되어 개인정보가 노출되는 경우를 홈페이지 설계 및 관리 미흡으로 구분할 수 있습니다.

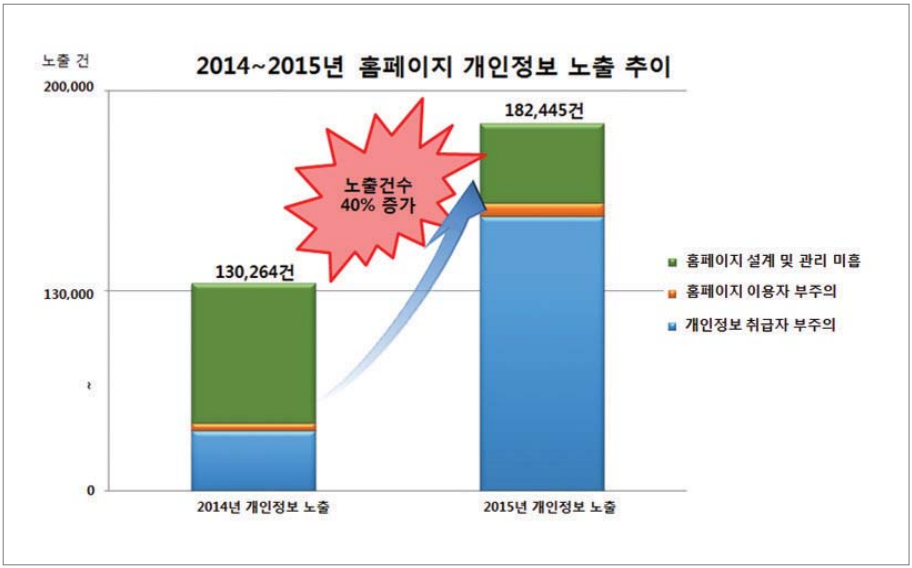
[표 2] 개인정보 노출의 원인

노출 원인	내 용
홈페이지 설계 및 관리 미흡	소스코드, URL, 홈페이지 취약점 등에 의해 개인정보가 노출되는 경우
첨부파일 노출	홈페이지에 개인정보가 포함된 첨부파일을 업로드 하는 경우
게시글 노출	홈페이지에 작성한 공지사항 및 댓글 등에 개인정보가 포함되어 있는 경우

[그림 2] 홈페이지 게시글 등록 시 개인정보 노출

개인정보 노출 현황을 분석해 보면,

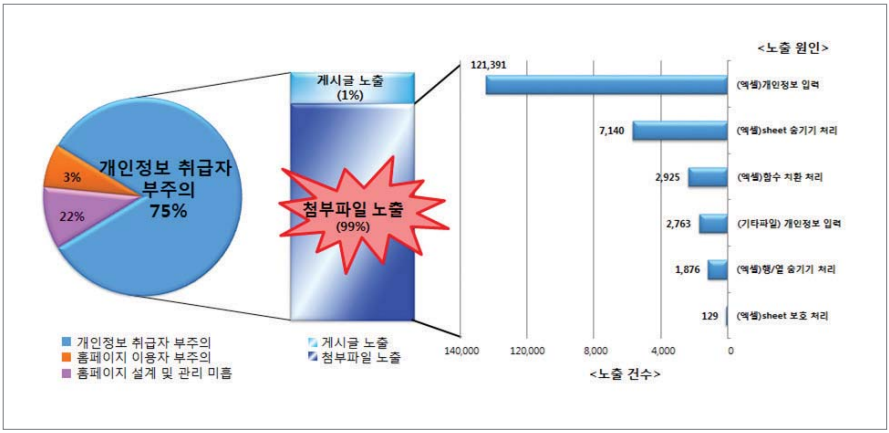
2015년에 홈페이지를 통한 개인정보 노출 건이 2014년 대비 약 40%(약 5만 건) 상승한 것을 볼 수 있습니다. [그림 3]에서 볼 수 있듯이 홈페이지 설계 및 관리 미흡은 지속적으로 감소되는 반면에, 파란색으로 표시된 개인정보 취급자 부주의로 인한 노출은 큰 폭으로 증가하고 있습니다.



[그림 3] 2014년~2015년 홈페이지 개인정보 노출추이

개인정보 노출 유형을 분석해 보면,

[그림 4]에서 볼 수 있듯이 개인정보 취급자 부주의로 인한 노출 건수가 전체의 75%를 차지하고 있습니다. 특히, 개인정보 취급자의 부주의로 인한 노출의 대부분이 개인정보가 포함된 첨부파일에 의해 발생하므로, 개인정보 취급자는 첨부파일을 등록하기 전에 해당 첨부파일 내에 개인정보가 포함되어 있는지 반드시 확인할 필요가 있습니다.



[그림 4] 2015년 개인정보 노출 원인 상세 분석한 노출 유형

[표 3] 공공/민간기관 주요 개인정보 노출 형태

대분류	중분류	주요 노출 형태	노출원인
공공기관	중앙행정기관	·참여마당 '자유게시판' 글에서 주민등록번호 노출 ·정보조회의 '일반정보' 글에서 운전면허번호 노출	게시글 노출
		·합격자발표 게시판의 'OO시험 합격자 명단' 첨부파일에서 여권번호 노출 ·임대안내 게시판의 신청서류 첨부파일에서 주민등록번호 노출 ·시험공고/공지사항 게시판의 '공채 임용유예자 명단' 첨부파일에서 주민등록번호 노출	첨부파일 노출
	지방자치단체	· '개별공시지가 이의신청' 첨부파일에서 주민등록번호 노출 ·과제검색 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출	첨부파일 노출
		·정보공개창 게시판의 '배출업소현황' 첨부파일에서 주민등록번호 노출 ·우리동소식 게시판의 '알선대상자 명단' 첨부파일에서 주민등록번호 노출 · 'OO시 선수명단' 파일에서 주민등록번호 노출 ·행정처분 명령서 파일에서 주민등록번호 노출	첨부파일 노출
	초중고	· '급식행정공개' , '가정통신문' 에서 주민등록번호 노출 ·행정실 게시판의 '운영위원회' 파일에서 주민등록번호 노출 ·부별업무자료의 '스카우트' 알집파일 내에 존재하는 첨부파일에서 주민등록번호 노출	첨부파일 노출
	대학교	·민원센터의 '학사/학적변동' 글에서 주민등록번호 노출 ·사이버강좌의 '개설강좌' 글에서 주민등록번호 노출	게시글 노출
		· '어학원 수강신청' 파일에서 외국인등록번호 노출 ·행정실 공지사항 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출	첨부파일 노출
		·OO대학교 관리자페이지에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
민간기관	여행업	· '여행예약확인 요청' 글에서 주민등록번호, 여권번호 노출 · '현금 영수증 요청' 글에서 주민등록번호 노출	게시글 노출
		·고객센터의 '질문과 답변' 글에서 주민등록번호 노출 ·이용안내의 '자주 묻는 질문 FAQ' 글에서 주민등록번호 노출	게시글 노출
	의료업	·건강상담의 '복약상담' 글에서 주민등록번호 노출	게시글 노출
		·정보광장의 '채용공고' 파일에서 주민등록번호 노출 ·요양급여비용 청구서 파일에서 주민등록번호 노출	첨부파일 노출
		·건강진단 결과표에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
	협회	· '개인성적기록' 조회 게시판에서 주민등록번호 노출 · '참가팀 소개' 게시판에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
		· '자원봉사신청서' 첨부파일에서 주민등록번호 노출 ·내용 증명서 파일에서 주민등록번호 노출	첨부파일 노출
	단체	·본회소개의 '회원명단' 글에서 주민등록번호 노출	게시글 노출
		·자료실 게시판의 '경매실적' 첨부파일에서 주민등록번호와 외국인등록번호 노출 ·재단소개의 '정관/이사회' 첨부파일에서 주민등록번호 노출	첨부파일 노출

홈페이지 노출 유형별 조치방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법

- 가. URL(홈페이지 주소)에 개인정보 사용부분 삭제
- 나. 홈페이지 소스코드 내에 개인정보 삭제
- 다. 임시 저장 페이지의 올바른 처리 방법
- 라. 디렉터리 리스팅의 올바른 설정 방법
- 마. 관리자페이지의 올바른 구성 방법

2. 첨부파일이 포함된 게시글 노출 시 조치방법

- 가. 일반적인(HWP, DOC, XLS 등) 첨부파일인 경우
- 나. 이미지 형식(이미지형 PDF, 이미지파일 등)의 첨부파일인 경우

3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법

4. 검색엔진에 저장된 페이지 삭제 방법 공통사항

- 가. 개인정보가 노출된 페이지 또는 파일 검색
- 나. 개인정보가 있는 검색엔진 캐시페이지 삭제요청
  - 구글(Google)에 노출된 개인정보 삭제 방법
  - 네이버(Naver)에 노출된 개인정보 삭제 방법
  - 다음(Daum)에 노출된 개인정보 삭제 방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출

홈페이지 설계 및 관리 미흡으로 인한 노출은 홈페이지 설계 당시 개인정보보호에 대해 충분히 고려하지 않고 홈페이지를 구축하여 개인정보가 노출되거나, 비공개 페이지에 대한 접근 제한이 미흡해 인증우회를 통해 개인정보가 노출되는 경우입니다.

[표 4] 홈페이지 설계 및 관리 미흡으로 인한 노출 유형

노출 유형	내 용
설계 미흡	URL에 개인정보가 노출
	이용자 화면 소스코드에 개인정보가 노출
	게시글 작성 중 임시 저장 페이지에 개인정보가 노출
	디렉터리 리스팅의 잘못된 설정으로 인해 개인정보가 노출
관리 미흡	관리자페이지 접근제한 미흡으로 인해 개인정보가 노출

가. URL에 개인정보가 노출된 사례

홈페이지 내의 특정페이지 주소(URL) 식별자로 주민등록번호 등을 사용하여 개인정보가 노출된 경우입니다.

주민등록번호는 개인을 구분하는 식별자로 사용할 수 없습니다. 홈페이지의 설계 변경을 통해 개인을 식별하는 값으로 별도의 구분자를 사용하고, 웹브라우저 주소 표시줄에 접속 파라미터가 나타나지 않도록 하는 것이 좋습니다.

[그림 5] URL에 주민등록번호가 노출된 사례

나. 이용자 화면 소스코드에 개인정보가 노출된 사례

홈페이지 화면상으로는 게시글에 개인정보가 포함되어 있지 않지만, 해당 화면에서 마우스 오른쪽 클릭 후 [소스보기]를 하면 글을 작성한 사람의 개인정보 확인이 가능한 경우입니다.

[그림 6]에서와 같이 게시글 화면 상에는 제목, 이름, 내용만 보이지만, 오른쪽 마우스 클릭 후 소스보기를 하면 소스코드 내에 개인정보가 포함되어 있는 것을 확인 할 수 있습니다.

개인정보가 이용자의 화면 상에는 보이지 않더라도 소스코드 상에 존재할 경우 개인정보가 노출되므로 홈페이지 설계 및 관리 시 이에 대한 조치가 반드시 필요합니다.

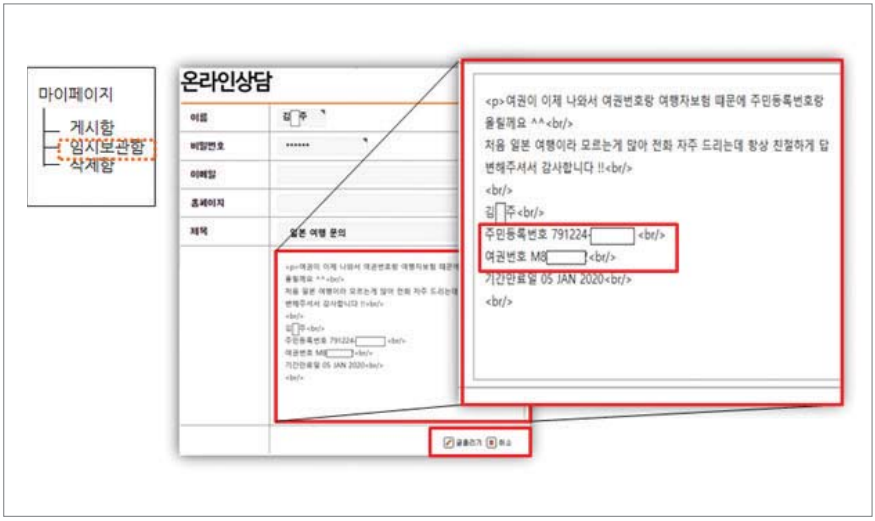
[그림 6] 소스보기에서 개인정보가 노출된 사례

다. 게시글 작성 중 임시 저장 페이지에 개인정보가 노출된 사례

홈페이지 설계 및 관리 미흡으로 인해 게시글의 임시 저장 페이지가 웹서버에 남아있어 해당 페이지의 개인정보가 노출된 경우입니다.

[그림 7]은 홈페이지 이용자가 여행사 홈페이지에 온라인상담 글을 작성하며 여행사에 제공할 개인정보 자료를 저장 완료하지 않고 임시 저장하여, 여행사 웹서버에 임시 저장 페이지가 남아있어 개인정보가 노출된 경우입니다.

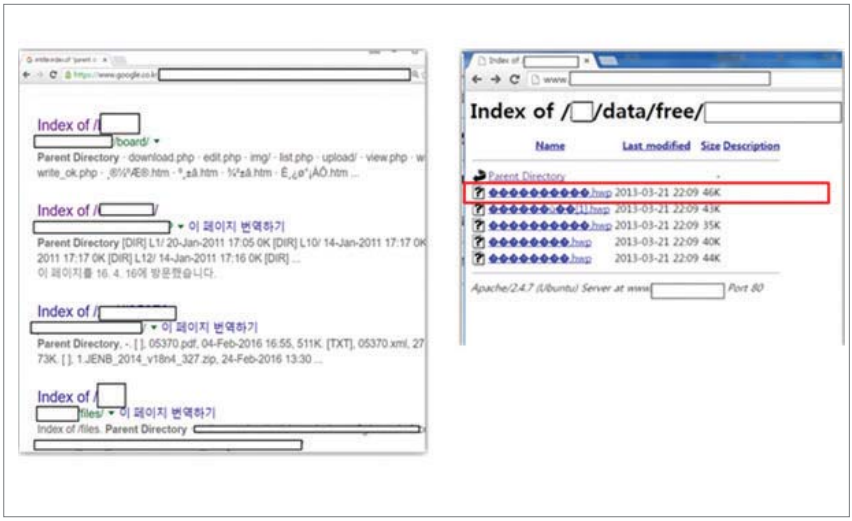
이러한 문제를 개선하기 위해 이용자가 홈페이지 접속을 종료하거나 게시글을 임시 저장한 후 일정기간이 지나면 임시 저장 페이지의 내용을 삭제하는 것이 좋습니다.



[그림 7] 임시보관함에 저장된 게시글 노출 사례

라. 디렉터리 리스팅의 잘못된 설정으로 인해 개인정보가 노출된 사례

디렉터리 리스팅 취약점은 개인정보의 노출 뿐 아니라 홈페이지 소스코드 전체가 노출되어 외부에 의한 해킹 등 2차적인 피해가 발생할 수 있고, 또 외부 검색엔진이 웹서버 디렉터리의 모든 파일들을 수집해 갈 수 있기 때문에 대량의 개인정보 노출이 발생할 수 있습니다.



[그림 8] 디렉터리 리스팅 취약점으로 개인정보가 노출된 사례

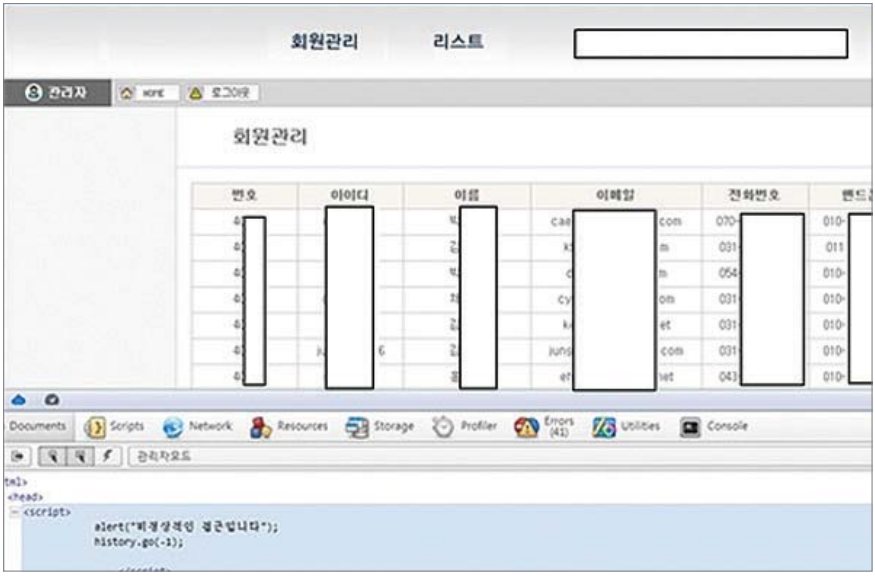
홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치방법 (예시)

Step 1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법(Ⅲ.1 참조)
Step 2. 검색엔진에 저장된 페이지 삭제 방법(공통사항)(Ⅲ.4 참조)

마. 관리자페이지 접근제한 미흡으로 개인정보가 노출된 사례

관리자페이지에 인증절차를 마련하지 않아 누구나 접근할 수 있도록 방치되어 개인정보가 노출되는 사례입니다. 관리자페이지는 홈페이지 가입회원 정보를 모두 볼 수 있는 페이지가 존재하기 때문에, 일반적인 노출 사례보다 더 많은 개인정보가 노출될 수 있습니다.

관리자페이지는 내부 네크워크에서만 접근할 수 있도록 접근 권한을 제한하는 것이 좋습니다. 불가피하게 외부에서의 접근이 필요할 경우에는 IP접근제어 또는 VPN 등을 이용하는 것이 좋습니다.



[그림 9] 관리자페이지 접근제한 미흡으로 노출된 사례

2. 첨부파일에 의한 노출

게시판에 첨부되는 엑셀, 한글문서, PDF, 텍스트파일 등 다양한 유형의 첨부파일에 개인정보가 노출되는 경우를 말합니다. 개인정보 취급자가 공지사항 등 게시판에 첨부파일을 업로드 하면서 첨부파일 내에 개인정보 포함여부를 확인하지 않고 게시할 경우 발생됩니다.

첨부파일 중에서도 엑셀(Excel) 파일은 정보를 많이 저장할 수 있는 이점이 있지만, 한번 노출이 되었을 때 대량의 개인정보가 노출되는 위험이 있습니다.

엑셀 파일로 인한 노출 사례를 살펴보면 엑셀 내 개인정보 입력, Sheet 숨기기, 함수 치환, 행/열 숨기기, Sheet 보호, 글자색을 배경색과 동일하게 작성, 메모 내 개인정보 입력 등의 순으로 개인정보 노출 빈도가 나타나며, 매우 다양한 유형으로 개인정보가 노출 되고 있음을 알 수 있습니다.

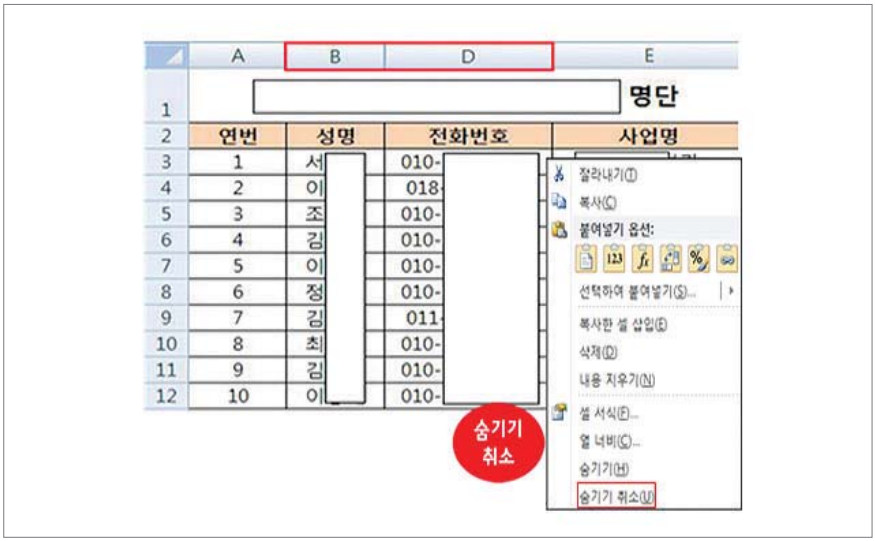
첨부파일로 인한 노출 대부분은 개인정보 취급자가 의도적으로 개인정보를 감추고자 한 목적이기 보다는 첨부파일 내 개인정보 포함 유무를 제대로 확인하지 않고 업로드하여 문제가 발생하는 경우가 많습니다.

[표 5] 엑셀 및 이미지 파일에 의한 노출 유형

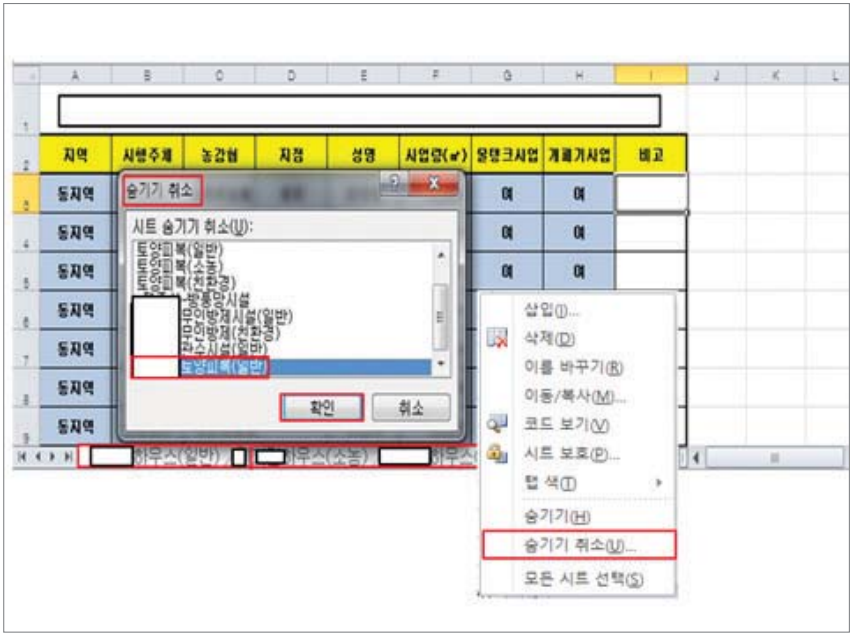
노출 유형	내 용
엑셀파일에 의한 노출	[숨기기] 기능에 의한 개인정보 노출
	시트보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보 노출
	함수 치환 후 원본 내용 미삭제로 인한 개인정보 노출
	[메모]기능으로 인한 개인정보 노출
	배경색과 같은 글자색으로 작성하여 개인정보 노출
	OLE 객체로 인한 개인정보 노출
이미지파일에 의한 노출	개인정보가 담긴 이미지형 PDF 파일에 의한 노출
	개인정보가 담긴 이미지 파일(JPG, GIF, BMP, PNG 등)에 의한 노출

가. [숨기기] 기능에 의해 개인정보가 노출된 사례

개인정보 취급자가 엑셀 파일에서 행/열 또는 Sheet [숨기기] 처리된 것을 확인 하지 못하여 개인정보 노출이 발생하는 경우입니다. 엑셀파일에는 행/열 또는 Sheet [숨기기] 기능이 있습니다. 개인정보가 포함된 행/열 또는 Sheet를 [숨기기] 처리한 파일을 열었을 때에는 개인정보가 바로 보이지는 않지만 행/열 또는 Sheet [숨기기 취소]를 할 경우 개인정보가 고스란히 포함된 것을 알 수 있습니다.



[그림 10] 열 숨기기 기능으로 개인정보 저장여부 미확인



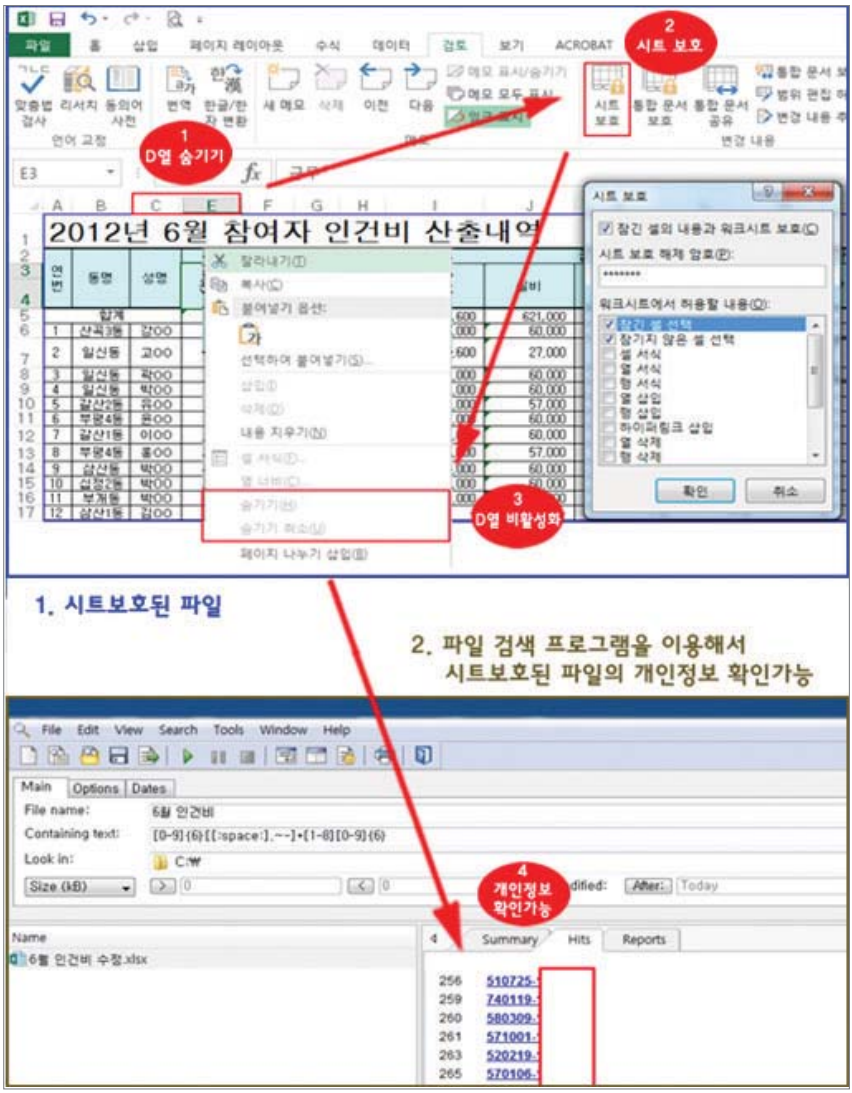
[그림 11] 시트 숨기기 기능으로 개인정보 저장여부 미확인

나. 시트보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보가 노출된 사례

개인정보 취급자가 엑셀의 시트보호 기능을 잘 못 활용하여 개인정보 노출이 발생하는 경우입니다. 엑셀의 시트보호 기능은 데이터를 암호화하는 기능이 아니라, 데이터가 변경되지 않도록 보호하는 기능입니다.

즉 숨기기 기능을 이용해 개인정보를 보이지 않도록 한 후 시트보호 기능으로 암호를 설정하더라도 숨겨진 데이터는 암호화되지 않아 개인정보 검색 시 노출되므로 주의해야 합니다.

따라서 파일검색 시 내용 확인이 되지 않도록 하려면 엑셀에서 제공하는 파일 암호설정 기능을 사용해야 합니다.



[그림 12] 시트보호로 개인정보가 보호되지 않는 사례

다. 함수 치환 후 원본 내용 포함으로 인해 개인정보가 노출된 사례

개인정보 취급자가 엑셀파일에서 개인정보가 포함된 셀을 LEFT나 REPLACE 등의 함수를 이용하여 주민등록번호 뒷자리를 *******(마스킹 처리) 하였으나 원본 자료가 삭제되지 않고 남아있어 개인정보가 노출된 경우입니다.

[그림 13]과 같이 함수 치환 기능을 사용하여 개인정보를 마스킹 처리하였지만, 마스킹 처리를 위한 원본 자료가 함께 존재하므로 함수 치환 기능으로는 개인정보를 보호할 수 없습니다.

따라서, 함수 치환 후에는 원본 자료를 반드시 삭제해야 합니다.

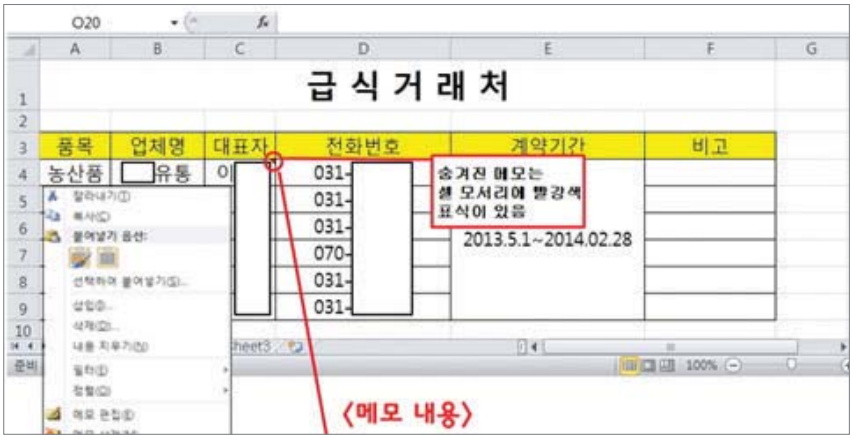
[그림 13] 함수 치환 후 원본자료 포함으로 인한 노출사례

라. [메모]기능에 포함된 개인정보 미삭제 사례

엑셀파일의 [메모] 기능 이용 시 메모 내용에 개인정보가 포함되어 개인정보 노출이 발생하는 경우입니다.

[그림 14]는 급식 거래처 명단에서 업무편의상 [메모] 기능을 사용하여 대표자 주민등록번호를 기록한 후, 메모 숨기기 기능으로 화면 상에 보이지 않게만 처리하여 개인정보가 노출된 사례입니다.

숨겨진 메모는 메모 숨기기 취소 기능을 통해 언제든지 내용을 다시 확인할 수 있으므로 개인정보가 포함되어 있을 경우 완벽하게 삭제하는 것이 좋습니다.



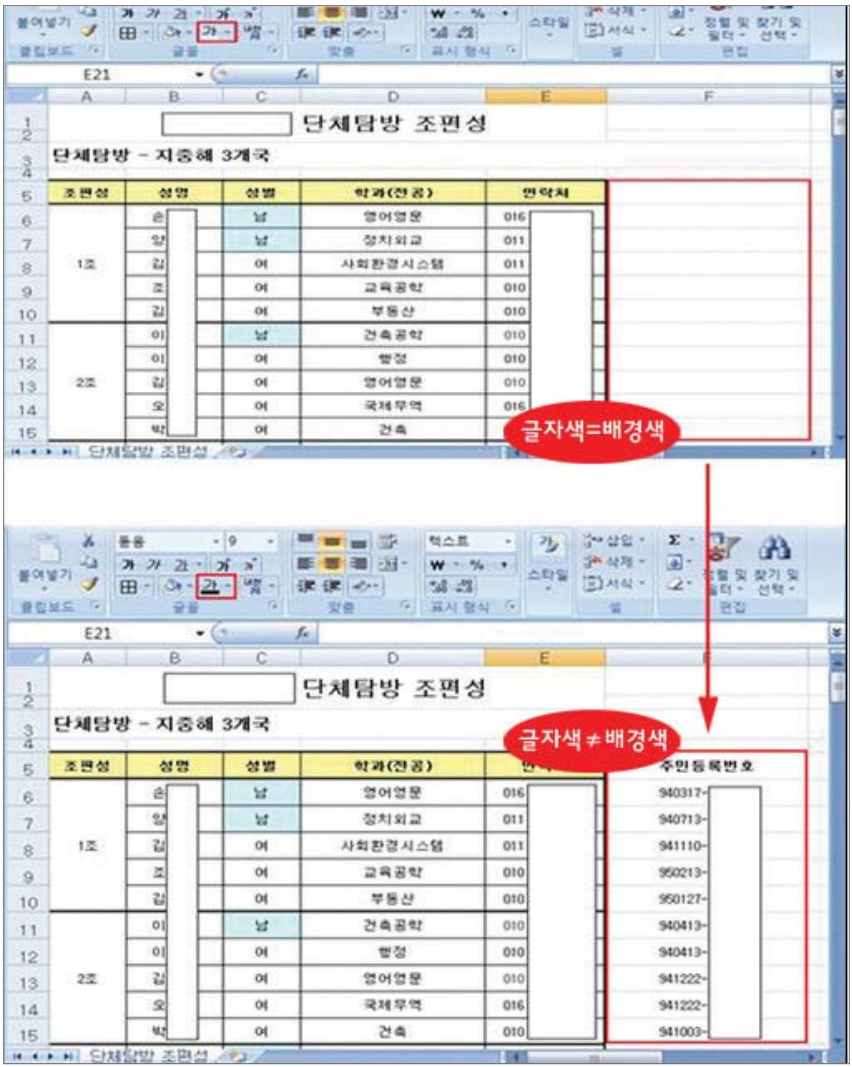
[그림 14] [메모] 내용에 개인정보가 포함된 사례

마. 배경색과 같은 글자색으로 작성하여 개인정보가 노출된 사례

파일 내 개인정보의 글자색과 배경색이 같아서 개인정보가 없는 것처럼 보이는 경우입니다. 육안으로는 보이지 않지만, 검색이나 드래그를 통해 없는 것처럼 보이는 글자들을 확인할 수 있습니다.

[그림 15]는 주민등록번호를 배경색과 같은 글자색(흰색)으로 작성하여, 웹사이트 이용자의 눈으로는 바로 확인할 수 없었으나, 개인정보 검색 프로그램을 통해서는 쉽게 찾아낼 수 있었던 사례입니다.

개인정보를 보이지 않게만 처리하는 것은 안전한 조치가 아닙니다. 개인정보를 식별하지 못하도록 마스킹 처리하거나 불필요한 개인정보는 삭제하는 것이 좋습니다.



[그림 15] 배경색과 같은 색상으로 글자색을 지정하여 개인정보 노출된 사례

바. OLE 객체로 인해 개인정보가 노출된 사례

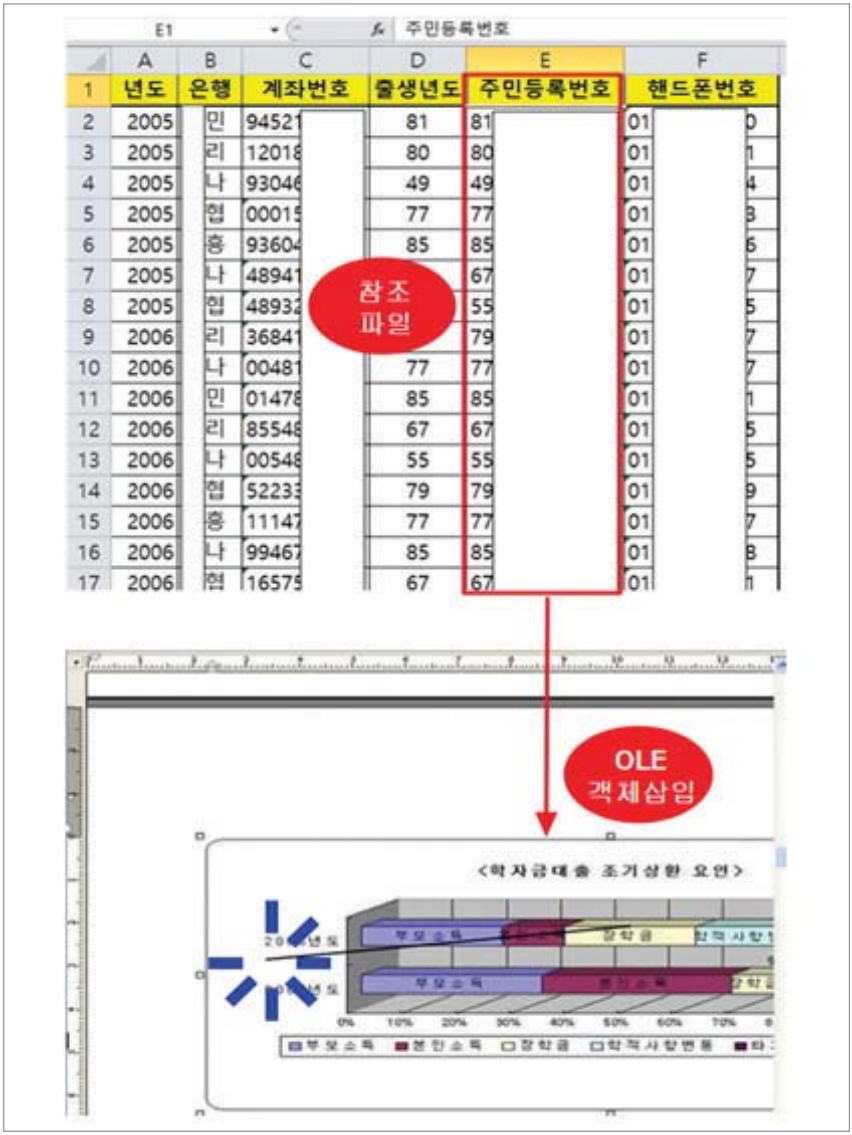
개인정보가 포함된 엑셀파일을 OLE(Object Linking and Embedding) 객체로 삽입한 후 해당 자료를 홈페이지에 게시하여 개인정보 노출이 발생하는 경우입니다.

[그림 16]과 같이 OLE 객체가 삽입되어 있는 그래프를 더블클릭하면 참조되어 있던 자료가 표시되는데, 그래프 상에 표시되지 않더라도 개인정보가 참조된 자료 내에 존재할 경우 무방비로 노출이 됩니다. 따라서 OLE 객체를 삽입할 때는 참조 파일 내에 나타내고자 하는 항목만 추려 작성해야만 합니다.

업무용 파일을 OLE객체와 연결할 경우 개인정보 등 원하지 않는 항목까지 포함 될 수 있으므로 반드시 주의가 필요합니다.

첨부파일에 의한 노출 시 조치방법 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 첨부파일이 포함된 게시글 노출 시 조치 방법(Ⅲ.2 참조)
Step 3. 검색엔진에 저장된 페이지 삭제 방법(공통사항)(Ⅲ.4 참조)



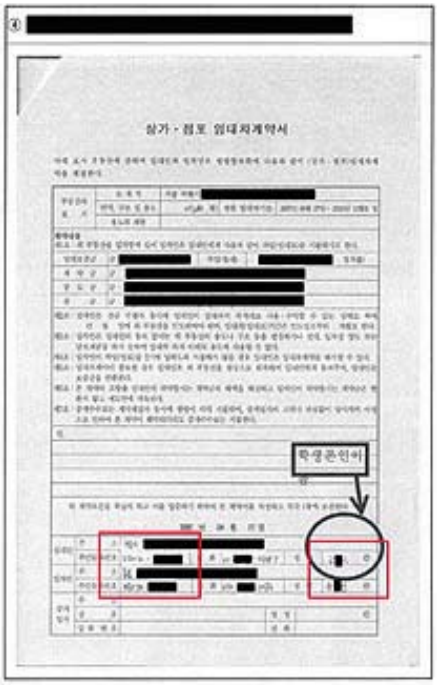
[그림 16] OLE 객체 내에 있는 개인정보 노출 사례

사. 개인정보가 담긴 이미지형 PDF 파일에 의해 노출된 사례

개인정보가 이미지형 PDF 파일에 포함되어 노출된 사례입니다.

일반 PDF 파일은 텍스트 기반으로 단어검색이 가능하여 첨부파일을 등록하기 전에 개인정보를 점검하는 것이 용이하지만, 이미지형 PDF 파일은 이미지를 PDF 형태로 저장하기 때문에 텍스트 검색 기능을 사용하기 어렵습니다.

따라서, 스캐너 등으로 생성된 이미지형 PDF 파일을 홈페이지에 등록할 경우에는 개인정보가 포함되어 있는지 육안으로 확인하는 것이 좋습니다.

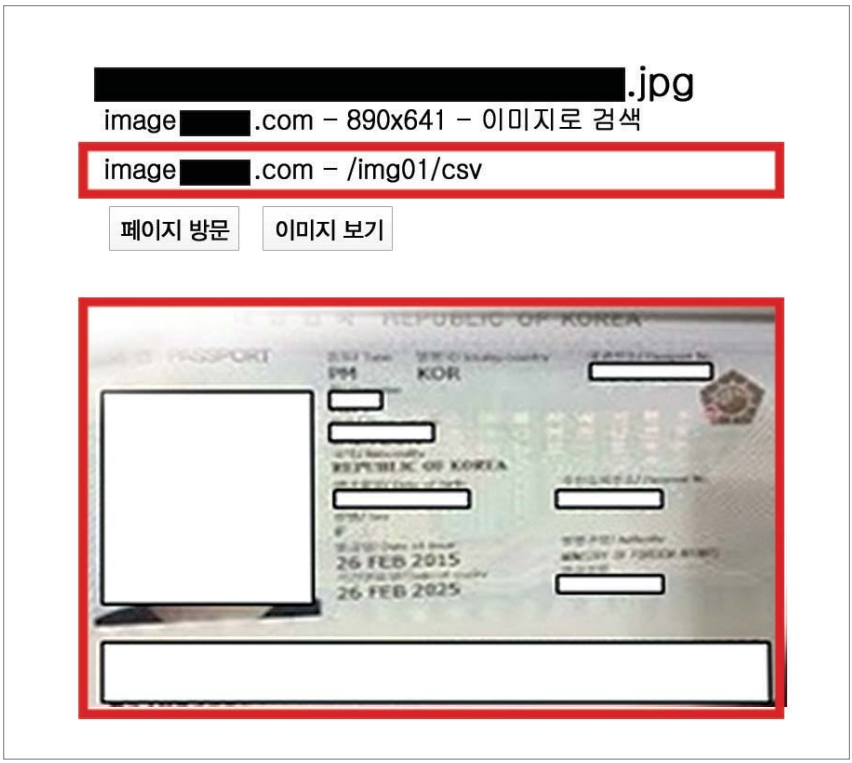


[그림 17] 이미지형 PDF 파일에 의한 노출 사례

아. 개인정보가 담긴 이미지 파일(JPG, GIF, BMP, PNG 등)에 의해 노출된 사례

개인정보가 이미지 파일(JPG, GIF, BMP, PNG 등)에 포함되어 노출된 사례입니다.

[그림 18]은 여행자보험 신청을 위해 여권사본을 여행사 홈페이지에 등록하였으나 디렉터리 리스팅 취약점에 의해 개인정보가 노출된 사례입니다. 개인정보가 포함된 이미지 파일의 노출을 방지하려면 디렉터리 리스팅 취약점 개선 및 개인정보가 포함된 이미지의 마스킹 처리가 필요합니다.



[그림 18] 웹서버에 저장된 여권사본 이미지 파일에 의한 개인정보 노출 사례

3. 게시글에 의한 노출

게시판을 통한 개인정보 노출 원인은 크게 두 가지 입니다. 첫째는 게시판에 게시글(공지사항, 민원 등)을 작성하면서 주민등록번호, 휴대폰번호 등이 포함되어 개인정보가 노출되는 경우이며, 둘째는 게시글에 대한 댓글을 작성하면서 개인정보가 노출되는 경우입니다.

[표 6] 게시글에 의한 노출 유형

노출 유형	내 용
게시글 노출	홈페이지 공지사항 등 게시글을 작성 시 개인정보가 포함 됨
댓글 노출	게시글에 대한 댓글을 작성 시 개인정보가 포함 됨

가. 게시글 작성에 의한 노출 사례

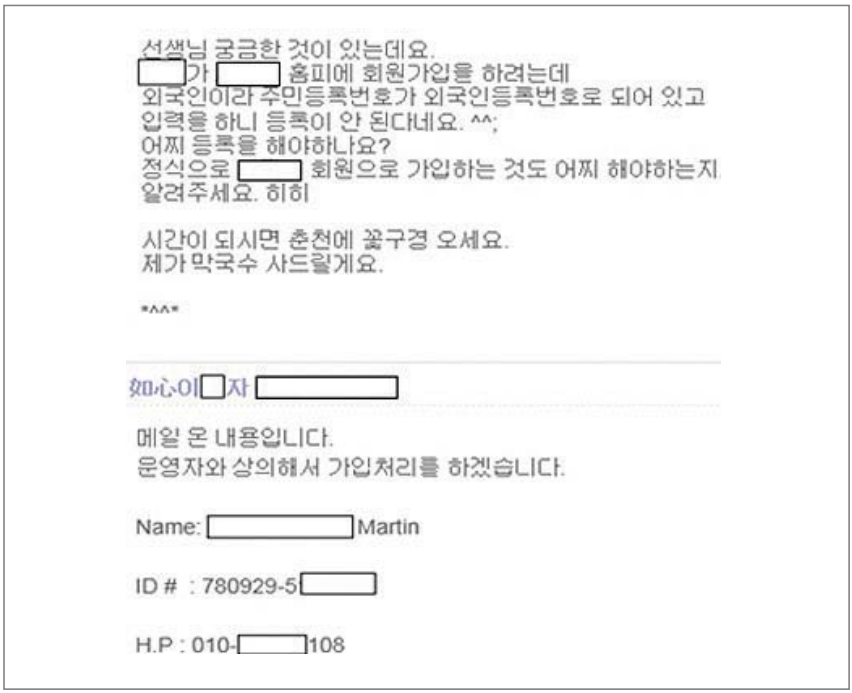
공지사항 등의 게시글 작성 시, 개인정보 취급자 및 홈페이지 이용자의 부주의로 게시글에 개인정보가 포함되어 노출되는 경우입니다.

[그림 19]는 홈페이지 이용자가 대학교 재학 중 취득한 자격증의 재발급을 요청하면서 본인의 연락처가 게시글에 노출되었던 사례입니다. 이 경우 홈페이지 이용자는 개인정보 부분과 연락처에 대해 **** 등으로 마스킹 처리를 하거나 해당 게시글을 비밀글로 전환하는 것이 필요합니다.

[그림 19] 홈페이지 이용자의 게시글에 개인정보가 노출된 사례

나. 댓글 작성에 의한 노출 사례

[그림 20]은 개인정보 취급자가 홈페이지 이용자의 요청사항에 대한 답변을 작성하면서 홈페이지 이용자의 개인정보가 노출되었던 사례로 개인정보 취급자의 상당한 주의가 필요한 경우입니다.

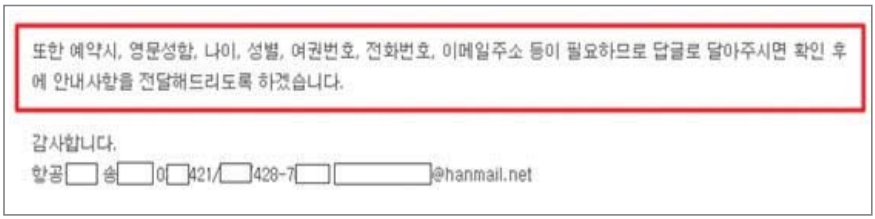


[그림 20] 개인정보취급자의 댓글에 개인정보가 노출된 사례

[그림 21]은 여행사에서 예약 업무처리를 목적으로 공개된 게시글에 개인정보 입력을 유도한 사례입니다.

개인정보 취급자는 업무편의를 위하여 홈페이지 이용자의 개인정보를 게시글에 공개적으로 작성하도록 유도해서는 안 됩니다. 업무처리를 위한 게시글은 홈페이지 이용자와 개인정보 취급자만 볼 수 있도록 비밀글로 처리하는 것이 좋습니다.

이 경우 개인정보 작성을 유도하는 안내글을 삭제하고, 공개된 게시글에 등록된 개인정보는 **** 등으로 마스킹 처리하거나 삭제해야만 합니다.



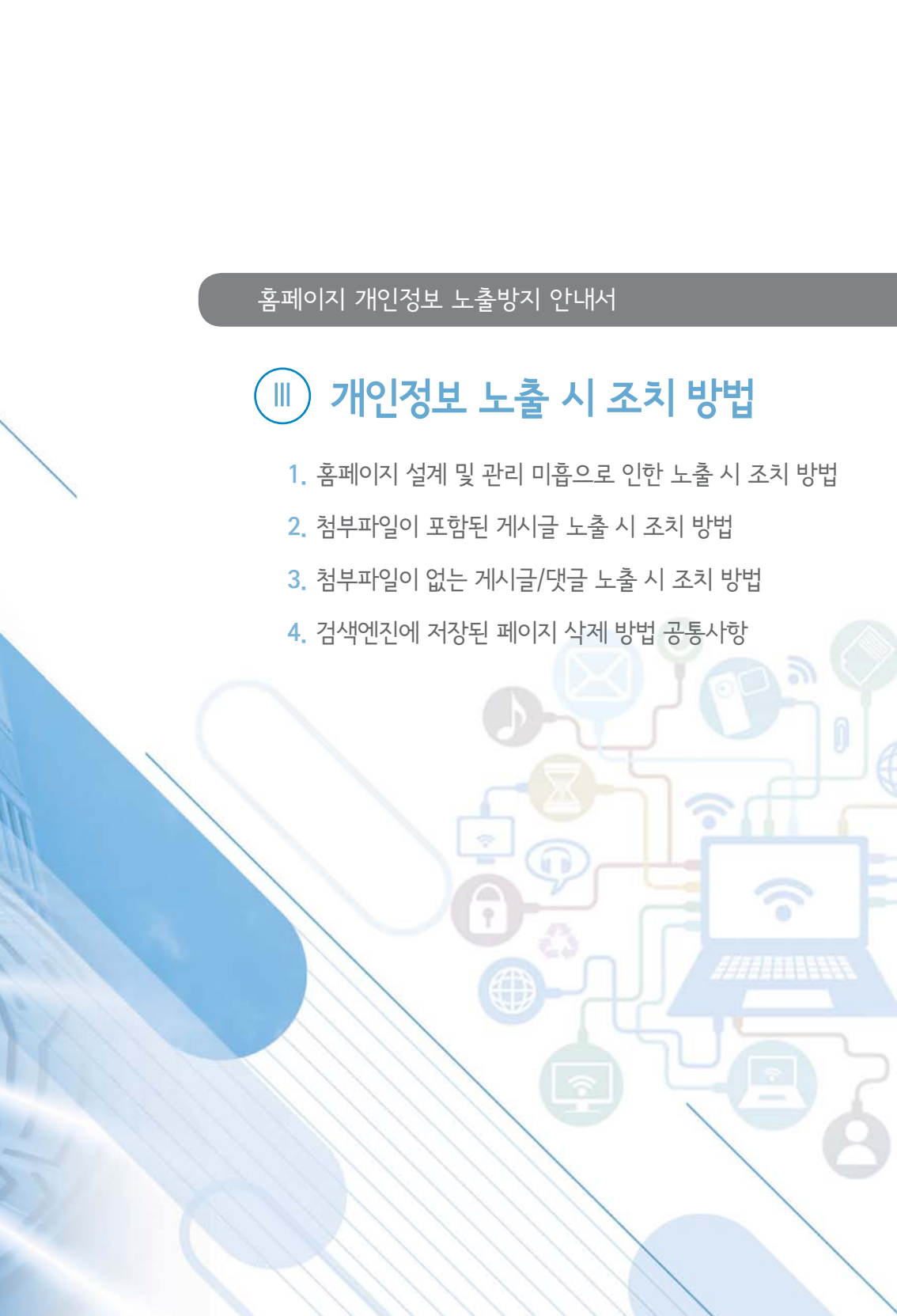
[그림 21] 빠른 업무처리를 위해 개인정보 노출을 유도한 사례

게시글/댓글 노출 시 조치방법 (예시)

Step 1. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법(Ⅲ.3 참조)
Step 2. 검색엔진에 저장된 페이지 삭제 방법(공통사항)(Ⅲ.4 참조)

Ⅲ 개인정보 노출 시 조치 방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법
2. 첨부파일이 포함된 게시글 노출 시 조치 방법
3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법
4. 검색엔진에 저장된 페이지 삭제 방법 공통사항



Ⅲ 개인정보 노출 시 조치 방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법

가. URL(홈페이지주소)에 개인정보 사용부분 삭제

홈페이지 설계 시 구분하기 위한 값으로 개인정보를 사용하는 경우 URL에 개인정보가 노출됩니다. 조치 방법은 개인을 구분하기 위한 값으로 개인정보를 사용하지 않고, 웹브라우저 주소 표시줄에 파라미터 값이 보이지 않도록 GET 방식보다는 POST 방식을 사용하는 것입니다.

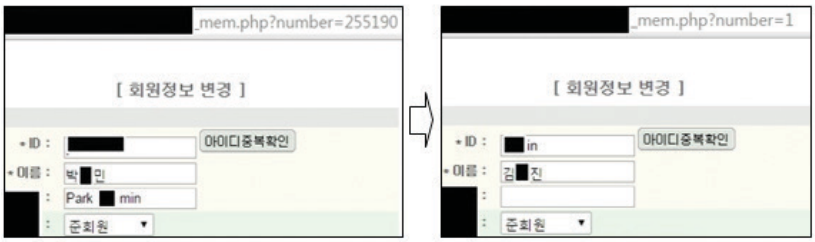
이 작업은 홈페이지의 프로그램 코드를 수정하는 것으로 개발 또는 운영 인력과 함께 처리해야 합니다.

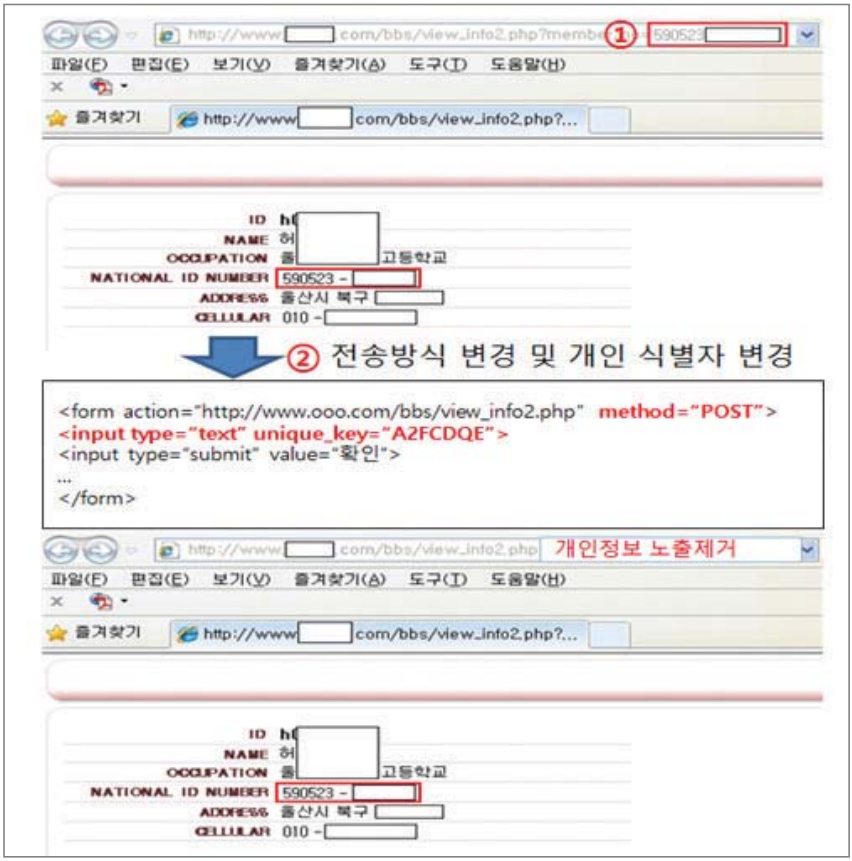
※ 홈페이지에서 개인 식별자의 변경은 많은 작업이 수반될 수 있으니 기술적인 부분에 대한 검토를 반드시 진행한 후 처리하도록 합니다.

참고사항

파라미터 값을 개인정보가 아닌 다른 값(숫자 등)으로 할당하는 경우에도, 하나의 파라미터를 습득 후 임의 변경을 통해 타인의 개인정보를 열람할 수 있습니다.

개인정보가 포함된 페이지는 인증절차를 마련하여 파라미터 임의 변경을 통한 개인정보 노출을 예방하는 것이 좋습니다.





[그림 22] URL에 개인정보가 노출된 경우 조치방법

처리절차 (예시)

Step 1. URL에 개인정보 노출여부 확인
Step 2. URL에 개인을 구분할 수 있는 값 정의 후 홈페이지에 적용
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

나. 홈페이지 소스코드 내에 개인정보 삭제

홈페이지 설계 시 화면에서는 보이지 않지만 소스코드 내부에 개인정보가 포함된 경우가 있습니다. 이 경우 간단히 소스 보기를 통해 개인정보가 노출될 수 있습니다.

이에 대한 조치 방법은 개인을 구분하기 위한 값을 변경하는 것으로, 해당 작업은 홈페이지 설계부분에 대한 전반적인 검토가 필요하기 때문에 개발 또는 운영자와 함께 빠르게 조치해 나가야 합니다.

[그림 23] 홈페이지 소스코드 내에 개인정보가 노출된 경우 조치 방법

처리절차 (예시)

Step 1. 인터넷 브라우저에서 소스보기를 통해 개인정보가 있는지 확인
Step 2. 업무 처리 시 불필요한 개인정보는 프로그램에서 삭제하고 꼭 필요한 정보는 암호화 처리
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조))

다. 임시 저장 페이지의 올바른 처리 방법

임시 저장 페이지는 홈페이지 이용자의 편의를 위해 제공하는 기능입니다. 홈페이지 이용자가 작성 중인 게시글의 내용이 없어지지 않도록 그 내용을 임시로 저장하는 것이지만, 작성 중인 게시글을 작성 완료하거나 또는 작성을 취소했을 경우에는 웹서버에 있는 임시 저장 페이지를 반드시 삭제해야 합니다.

임시 저장 페이지에서 개인정보가 노출되지 않도록 하기 위해서는 게시글 작성 완료 및 작성 취소 시 저장된 임시 페이지를 바로 삭제하고, 일정기간이 경과된 임시저장 페이지는 자동으로 삭제될 수 있도록 조치하는 것이 좋습니다.

소상공인, 중소사업자 및 비영리단체 대상 개인정보 보호 기술 지원

구분	내 용
지원내용	· 개인정보 보호조치 컨설팅 · 홈페이지 웹 취약점 점검 서비스 · 업무용PC 점검도구 제공 · 주민등록번호 미 수집, 암호화 조치 지원
절차/방법	· 우편, FAX, 이메일, 홈페이지
온라인신청	· 개인정보보호 종합포털(www.privacy.go.kr) 〉 사업자 〉 개인정보보호 기술지원
문의처	· 한국인터넷진흥원 개인정보보호 기술지원센터 (☎ 118)

※ 본 내용은 참고사항이며 해당 여부는 서비스 신청 후 심사기관의 별도 조사를 통해 확인 바랍니다.

라. 디렉터리 리스팅의 올바른 설정 방법

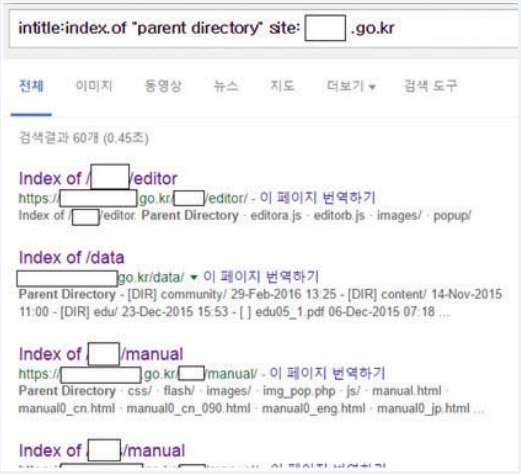
디렉터리 리스팅 설정은 웹브라우저를 이용한 자료 관리를 위해 주로 사용하지만 홈페이지의 모든 디렉터리를 볼 수 있어 보안성 면에서 취약한 서버설정입니다. 서버에 있는 모든 경로에 직접 접근이 가능하므로 회원 개인정보와 관련된 파일들이 외부로 노출될 수 있습니다.

디렉터리 리스팅 취약점이 발견될 경우, 웹 서버에서 해당 디렉터리를 외부에서 읽지 못하도록 디렉터리의 설정을 변경하여야 합니다.

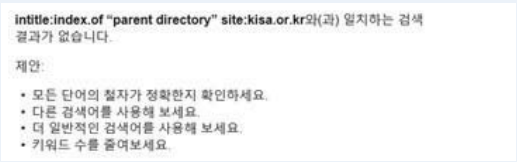
디렉터리 리스팅

서버관리자가 사이트 테스트 목적으로 사용하는 설정으로 브라우징하는 모든 디렉터리를 볼 수 있지만 그만큼 보안에 매우 취약한 서버설정입니다. 서버에 있는 모든 경로에 직접 접근이 가능하므로 회원 개인정보에 대한 파일이 외부로 노출될 수 있습니다.

☑ **디렉터리 리스팅 검색방법**



[그림 24] 디렉터리 리스팅 취약점이 있는 홈페이지의 검색 예시



[그림 25] 디렉터리 리스팅 취약점이 없는 홈페이지의 검색 예시

UNIX 또는 LINUX 환경

☑ Apache : httpd.conf 파일에서 indexes 문자열 제거

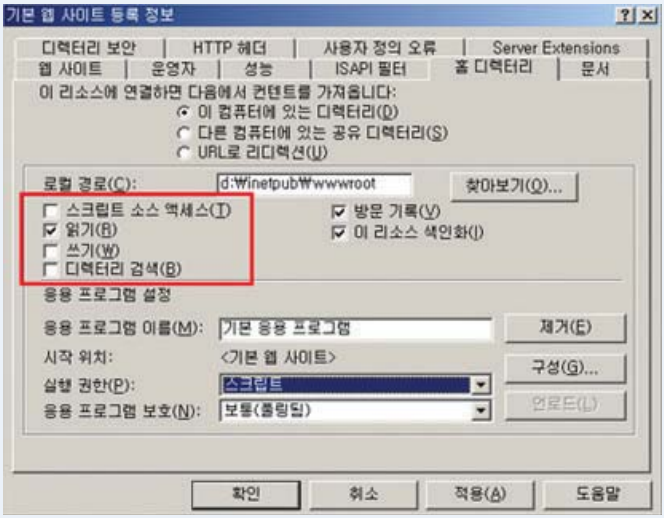
```
<Directory "/user/local/server/apache/htdocs">
        Options Indexes
</Directory>
```

☑ Tomcat : web.xml 파일에서 param-value false 로 설정변경

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

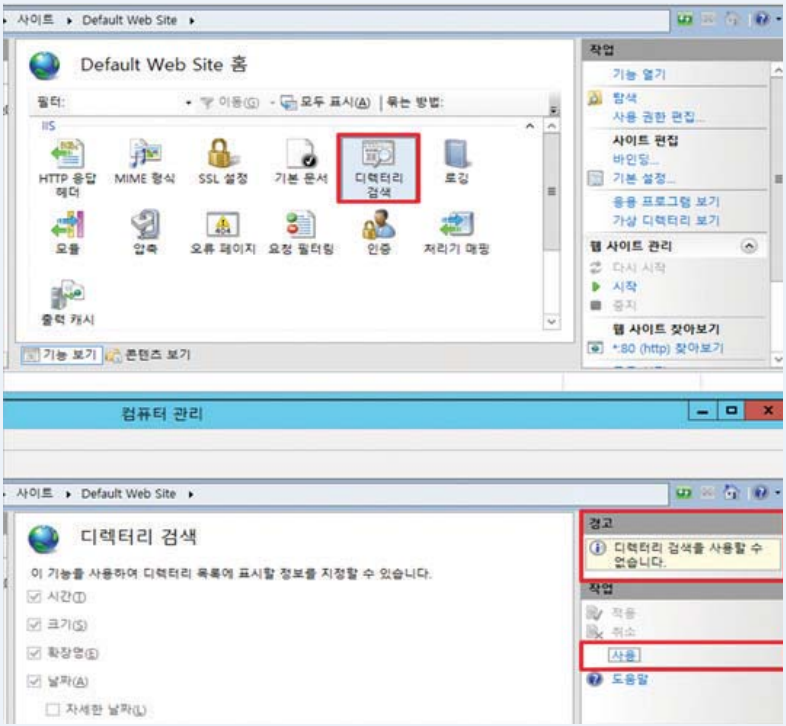
윈도우 IIS(Internet Information Service) 환경

☑ IIS 6.x 이하 : 제어판 → 관리도구 → 인터넷 서비스 관리자
→ 기본 홈페이지 의 속성에서디렉터리 검색 부분을 비활성화



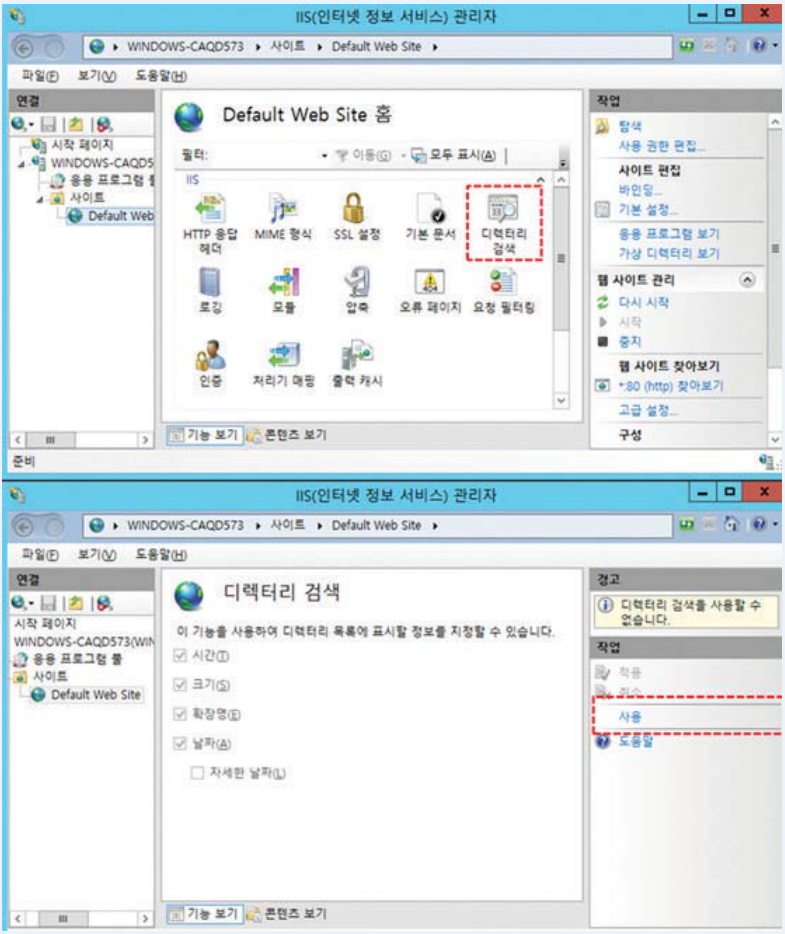
[그림 26] IIS 6.x 이하에서 디렉터리 리스팅 방지 설정

☑ IIS 7.x : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 홈페이지 홈 → 디렉터리 검색을 더블클릭 후 속성에서 우측 작업창에서 사용 해제



[그림 27] IIS 7.x 에서 디렉터리 리스팅 방지 설정

IIS 8.x : 제어판 → 시스템 및 보안 → 관리도구 → IIS(인터넷 정보서비스) 관리자 → 사이트 → 기본 홈페이지 홈 → 디렉터리 검색을 더블클릭 후 속성에서 우측 작업창에서 사용 해제



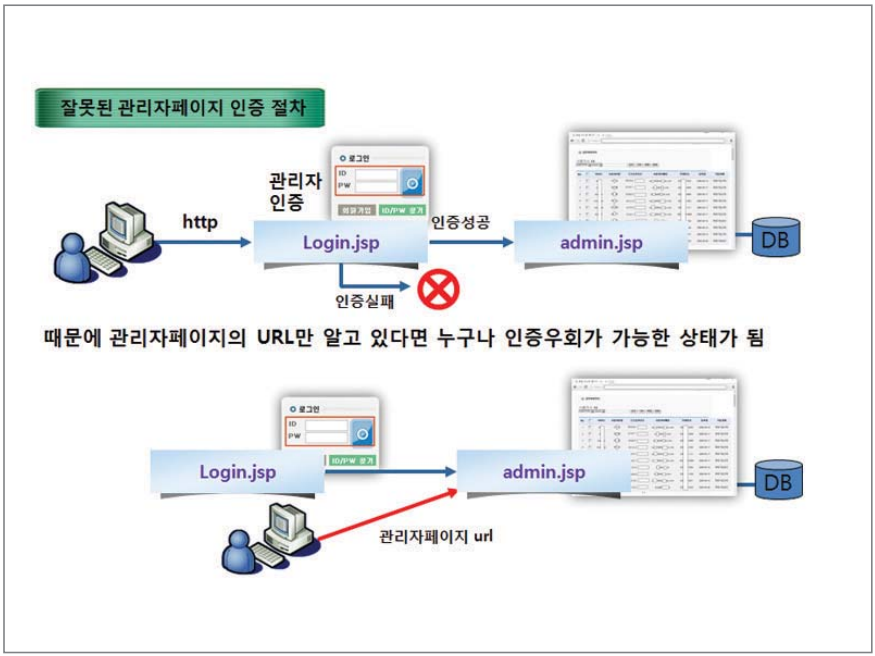
[그림 28] IIS 8.x 에서 디렉터리 리스팅 방지 설정

마. 관리자페이지의 올바른 구성 방법

관리자페이지의 접근권한 관리가 미흡한 경우 서비스 이용자들의 개인정보가 노출되어 해당 정보가 악용되는 피해가 발생할 수 있습니다. 홈페이지에 관리자페이지의 주소를 링크로 만들어서는 안 되며, 관리자페이지의 주소를 쉽게 추측 가능한 주소로 사용하지 말아야 합니다.

또한, 관리자페이지 접근을 위한 인증정보(세션 정보 등)는 처음 로그인화면 뿐 아니라 관리자페이지 전체에서도 모두 체크하도록 하여 제3자가 인증 없이 관리자페이지에 접근하는 것을 방지하도록 합니다.

마지막으로 관리자페이지를 외부에서 접속할 때는 전용선이나 가상사설망(VPN)을 이용하는 것이 좋습니다.



[그림 29] 관리자페이지 구성

외부 검색엔진의 이해

검색엔진은 인터넷에 공개된 홈페이지의 정보를 수집하여 홈페이지 이용자들이 원하는 정보를 쉽게 찾아주는 기능을 제공합니다. 검색엔진의 크롤러(수집기)는 인터넷의 홈페이지를 돌아다니며 정보를 수집하여 검색엔진 DB에 저장합니다. 이용자가 검색엔진에 (1) 질의어를 전달하면 (2) 검색엔진은 검색엔진 DB에서 질의어를 색인하여 (3) 검색결과를 이용자에게 전달합니다. 이 과정에서 다양한 정보가 검색엔진 DB에 수집되며 개인정보나 비공개 자료도 포함될 수 있습니다.

[그림 30] 검색엔진의 질의어 검색 과정

검색엔진에 수집되는 기관 홈페이지 내용 확인

일반적으로 공공기관은 홈페이지를 통해 기관 업무를 이용자들에게 서비스하거나, 정보를 제공하는 용도로 사용하고 있습니다. 홈페이지 이용자들은 자신이 필요로 하는 내용을 검색엔진을 통해 검색할 수 있습니다. 이처럼 기관 담당자들이 홈페이지에 게시하는 글이나 자료가 외부 검색엔진을 통해 검색될 수 있으므로, 검색엔진을 통해 수집되고 있는 기관 홈페이지의 내용을 파악하고 있어야 개인정보 노출을 예방할 수 있고, 노출 발생 시 신속히 개인정보가 포함된 자료를 검색하여 삭제조치 할 수 있습니다.

웹마스터 도구 사용방법 숙지

홈페이지에 개인정보가 포함된 자료가 게시되었다면 즉시 해당 자료를 삭제조치 해야 하며, 외부 검색엔진이 해당 자료를 수집해갔는지 확인해봐야 합니다. 이를 위해서는 국내/외 포털사이트 및 검색엔진에서 노출된 자료를 삭제하는 방법을 숙지해야 합니다(Ⅲ.4 참조).

검색엔진에 저장된 페이지

키워드 등을 사용하여 검색한 결과페이지에는 두가지 종류의 페이지가 있습니다. 하나는 현재 운영중인 페이지 정보이고, 다른 하나는 검색엔진이 이전에 수집하여 보관하고 있는 캐시된 페이지 정보입니다.

따라서, 개인정보 노출시 현재 페이지의 정보만 수정한다고 해서 노출이 차단되지 않으며, 캐시된 페이지까지 모두 삭제가 되어야 노출이 차단됩니다.

2. 첨부파일이 포함된 게시글 노출 시 조치 방법

첨부파일에 개인정보가 포함되어 노출되는 유형은 일반적인 문서파일(HWP, DOC, XLS, PPT 등)에 의한 노출과 이미지 형식의 파일에 의한 노출로 구분할 수 있습니다. 첨부파일에 의한 노출 발생 시 일반 문서파일인지 이미지 형식의 파일인지 먼저 확인하고 조치를 취해야 합니다.

가. 일반적인(HWP, DOC, XLS 등) 첨부파일인 경우

첨부파일에 개인정보가 포함되어 노출된 경우에는 해당 게시글을 비공개로 전환한 후에 첨부파일을 먼저 삭제한 후 첨부파일 내에 있는 개인정보를 삭제하거나 123456-1****** 와 같이 마스킹 처리하여 재등록 합니다. 또한, 웹서버에서 첨부파일이 저장되어 있는 디렉터리(예:/홈페이지/첨부파일폴더)를 찾아서 개인정보가 있는 파일을 반드시 삭제해야 합니다. 개인정보를 삭제 또는 마스킹 처리한 파일을 재등록 했어도 웹서버에는 기존 파일이 남아있어 외부에 지속적으로 노출될 수 있습니다.

[그림 31] 첨부파일 내 개인정보 노출 시 조치 절차

마지막으로, 노출된 페이지의 처리가 끝난 후에는 항상 검색엔진에서 해당 페이지가 수집되었는지 확인하고, 수집된 페이지가 있을 시 삭제요청을 하여야 합니다.

처리절차 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 첨부파일의 개인정보 삭제 또는 123456-1******와 같이 마스킹 처리하여 재등록
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

나. 이미지 형식(이미지형 PDF, 이미지파일 등)의 첨부파일인 경우

이미지 형식(이미지형 PDF, JPG, PNG, TIF 등)의 첨부파일이 노출되었을 경우에는 해당 게시글을 비공개로 전환한 후에 첨부파일을 먼저 삭제하거나, 이미지를 편집할 수 있는 소프트웨어(그림판 등)를 사용하여 개인정보 부분을 마스킹 처리 한 후 재등록하도록 합니다.

[그림 32] 이미지형 마스킹 처리 예시

처리절차 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 이미지형 첨부파일의 삭제 또는 개인정보 부분 이미지를 지운 후 재등록(마스킹처리)
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법

개인정보 취급자/홈페이지 이용자가 작성한 게시물에 개인정보가 포함되어 있는 경우, 게시물을 비공개 전환하여 개인정보가 노출되지 않도록 임시조치하고, 해당 페이지를 삭제하거나 개인정보를 123456-1******와 같이 마스킹 처리 한 후 재등록해야 합니다.

[그림 33] 게시글/댓글 내 개인정보 노출 시 조치 절차

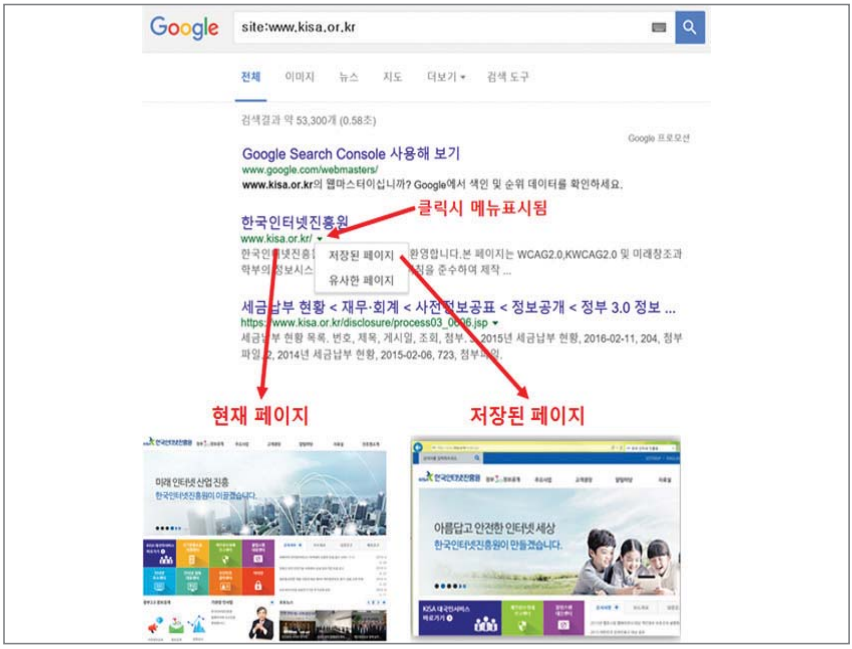
마지막으로, 노출된 페이지의 처리가 끝난 후에는 항상 검색엔진에서 해당 페이지가 수집되었는지 확인하고, 수집된 페이지가 있을 시 삭제요청을 하여야 합니다.

처리절차 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 게시글 삭제 또는 개인정보를 123456-1******와 같이 마스킹처리하여 재등록
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

4. 검색엔진에 저장된 페이지 삭제 방법 공통사항

개인정보가 노출되었을 경우 노출된 페이지에 있는 개인정보를 삭제하였어도, 검색엔진은 삭제하기 이전의 홈페이지 정보를 저장하고 있으며, 이를 캐시페이지라고 합니다.



[그림 34] 검색엔진에 저장된 페이지 확인 방법

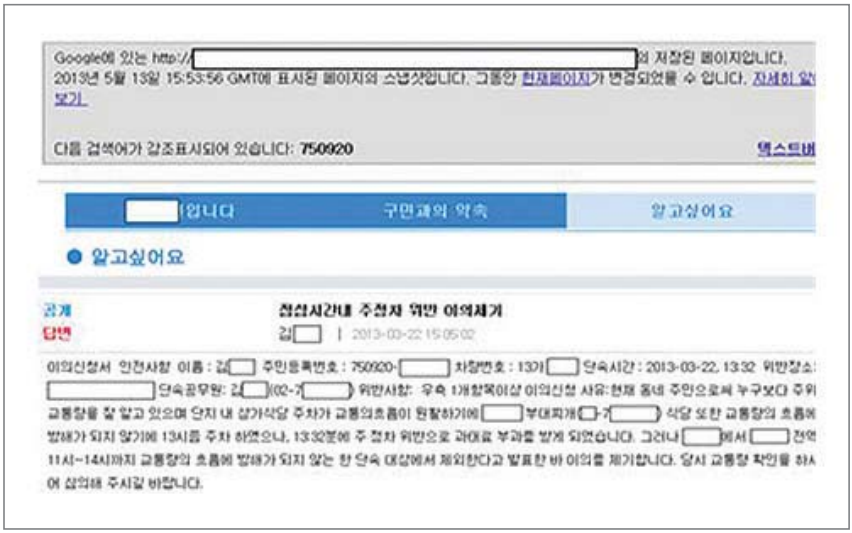
저장된 페이지(캐시페이지)의 갱신(Update)은 별도의 삭제 요청을 하지 않는 경우, 검색엔진 종류에 따라 몇 주에서 수개월이 소요됩니다.

따라서, 개인정보가 노출되었을 경우에는 노출된 홈페이지나 첨부파일에 대한 개선조치 이후에 검색엔진에 수집된 홈페이지를 삭제해 달라는 요청을 하는 것이 좋습니다.(삭제 요청 시 1일~3일 소요)

가. 개인정보가 노출된 페이지 또는 파일 검색

개인정보가 노출된 페이지를 삭제 또는 수정하였을 경우 검색엔진에서 노출된 페이지의 URL 또는 노출된 값을 이용하여 페이지를 검색합니다. (참고3. 구글 웹 마스터 도구 사용법 참조)

검색의 결과에서 [그림 35]와 같이 캐시페이지에 개인정보가 존재할 경우에는 검색엔진에 해당 페이지를 삭제해 달라는 요청을 해야 합니다.



[그림 35] 검색엔진 캐시에 저장된 개인정보 노출내역 확인

나. 개인정보가 있는 검색엔진 캐시페이지 삭제요청

각 검색엔진에는 캐시된 페이지에 대해 삭제를 요청하는 별도의 홈페이지를 제공하고 있습니다.

각 검색엔진별로 삭제 요청을 위한 접속 URL 은 아래 표와 같습니다.

[표 7] 검색엔진별 캐시페이지 삭제요청 주소

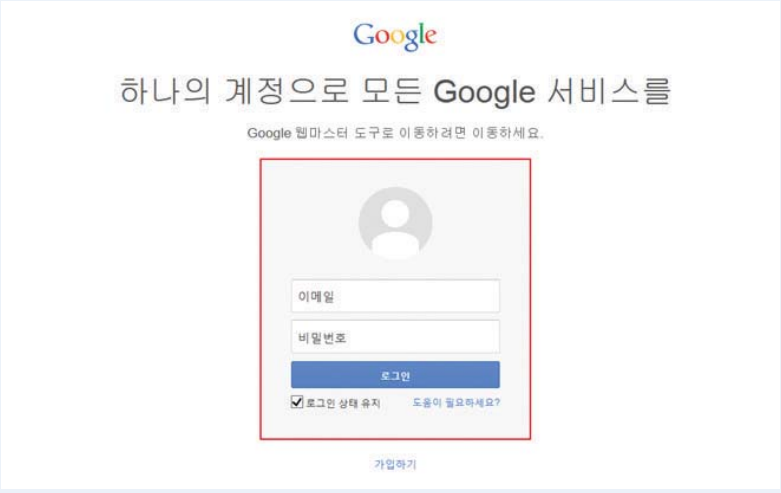
검색엔진	명칭	삭제요청 주소
구글(Google)	오래된 컨텐츠 삭제	https://www.google.com/webmasters/tools/removals
네이버(Naver)	삭제 문의 고객센터	https://help.naver.com/support/home.nhn
다음(Daum)	권리침해 신고센터	https://cs.daum.net/redbell/top.html

그러면 검색엔진별로 삭제를 요청하는 절차를 말씀드리겠습니다.

구글(Google)에 노출된 개인정보 삭제 방법

구글(Google)의 오래된 페이지 삭제(https://www.google.com/webmasters/tools/removals)화면에 접속합니다.

☑ **1단계 계정으로 로그인 합니다.**



[그림 36] 구글 계정 로그인 화면

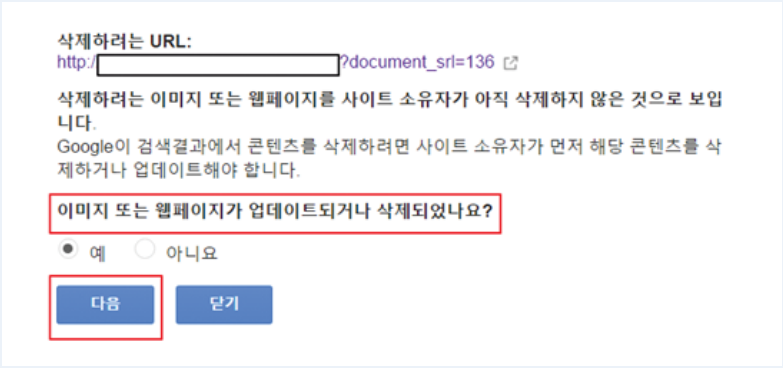
2단계 (삭제할 URL 입력)

[그림 37] 삭제 요청하기 클릭

3단계 (URL 분석 결과, 홈페이지가 삭제된 경우)

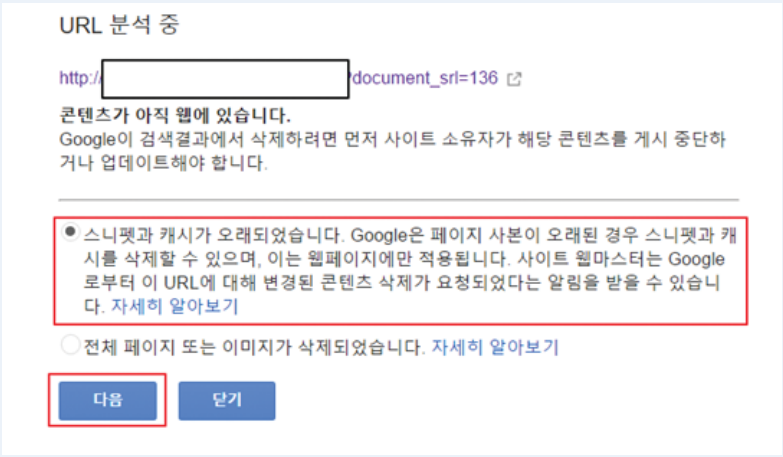
[그림 38] 삭제 요청 클릭

4단계 (URL 분석 결과, 홈페이지에 노출내용은 지웠으나, 페이지가 아직 남아 있는 경우)



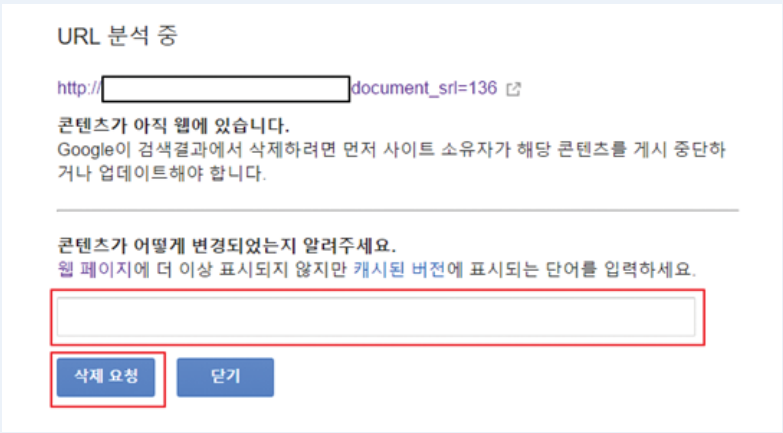
[그림 39] '다음' 으로 진행하기 클릭

5단계 (스니펫 및 캐시 삭제)



[그림 40] '다음' 으로 진행하기 클릭

6단계 (삭제하고자 하는 텍스트 입력)



[그림 41] 삭제 요청 클릭

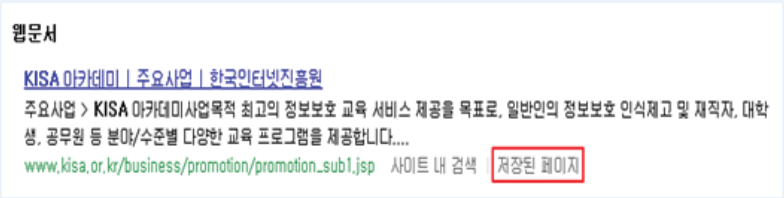
7단계 (삭제 요청 완료, 반영까지 일주일 정도 소요)

[그림 42] 구글(Google) 삭제 확인 및 처리

네이버(Naver)에 노출된 개인정보 삭제 방법

네이버(Naver)의 삭제 문의 고객센터(https://help.naver.com/support/home.nhn)에 접속합니다.

1단계 (삭제할 캐시 페이지 선택)

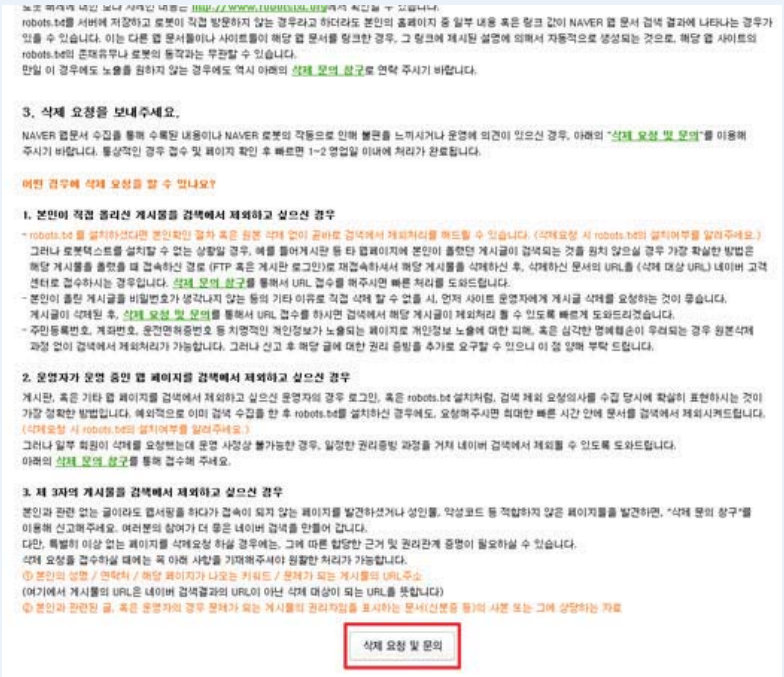


[그림 43] 네이버(Naver) 저장된 페이지 클릭

2단계 (웹문서 삭제 요청 방법 선택)

[그림 44] 네이버(Naver) 웹 문서 삭제 요청 방법 클릭

3단계 (삭제 요청)



[그림 45] 네이버(Naver) 삭제 요청 및 문의 클릭

4단계 (삭제 사유 선택)

[그림 46] 네이버(Naver) 검색 결과 제외 요청하기 화면

5단계 (삭제요청)

[그림 47] 네이버(Naver) 삭제 요청 문의 접수 화면

다음(Daum)에 노출된 개인정보 삭제 방법

다음(Daum)의 권리침해 신고센터(https://cs.daum.net/redbell/top.html) 에 접속합니다.

개인정보가 다음(Daum)에 노출된 경우, 다음(Daum) 고객센터 권리침해 신고를 통해 삭제를 요청할 수 있습니다.

[그림 48] 다음(Daum) 고객센터에서 신고하기 클릭

☑ 1단계 (온라인 접수 방법 선택, 오프라인 신청도 가능함)

[그림 49] 다음(Daum) 개인정보 침해 신고 관련 삭제 접수 방법 선택

2단계 (본인 확인)

[그림 50] 다음(Daum) 실명인증 방법 선택

3단계 (삭제 요청)

[그림 51] 다음(Daum) 개인정보침해 신고 삭제 요청 화면

Ⅳ 개인정보 노출 사전에 예방하세요

key 1. 첨부파일을 업로드하기 전에 개인정보가 있는지 확인하는 것이 좋습니다.

key 2. 관리자페이지는 안전하게 보호하세요.

key 3. 주기적으로 홈페이지의 개인정보 노출여부를 점검하는 것이 좋습니다.

key 4. 게시글에 비공개 설정 기능이 있는 것이 좋습니다.

key 5. 게시글 작성 시 개인정보 노출주의에 대한 안내를 하는 것이 좋습니다.

>> **용어 정의**

Ⅳ 개인정보 노출 사전에 예방하세요

Key 1

첨부파일을 업로드하기 전에 개인정보가 있는지 확인하는 것이 좋습니다.

☞ 업무자료를 공개할 경우, 새로운 파일에 공개할 부분만 복사해서 게시합니다.
☞ 첨부 문서에서 개인정보의 포함여부 확인 후 게시합니다.
  – 숨겨진 Sheet/행/열에 개인정보가 있는지 확인합니다.
  – 문서에 포함된 이미지에 개인정보가 있는지 확인합니다.
  – OLE 객체(그래프 등)는 더블클릭 후 원본자료에 개인정보가 있는지 확인합니다.
☞ 개인정보 검색 제품이 설치된 사용자 PC는 개인정보 포함여부를 점검 후 게시합니다.

Key 2

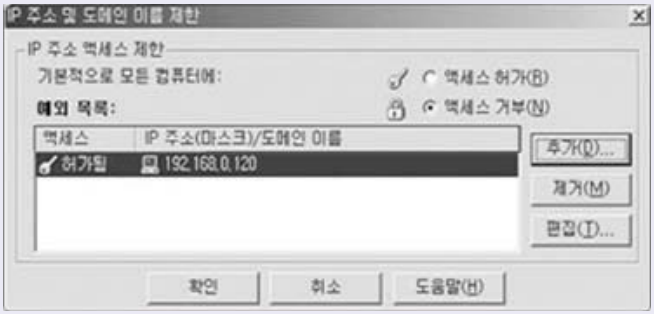
관리자페이지는 안전하게 보호하세요.

☞ 관리자 페이지에 외부접속이 필요할 경우, 전용선이나 가상사설망(VPN)을 이용합니다.
☞ 관리자 페이지는 관리자만 접속할 수 있도록 IP를 제한합니다.
☞ 관리자 페이지는 보안서버(SSL)를 적용하여 통신구간을 암호화합니다.
☞ 관리자 페이지는 인증된 관리자만 접속할 수 있도록 임의 접근을 제한합니다.
☞ 관리자 페이지의 주소에 추측 가능한 단어(admin, manager 등) 사용을 자제합니다.

관리자페이지 접근제한의 설정

1. IIS 웹서버(윈도우즈 서버)의 경우

– '설정 〉 제어판 〉 관리도구 〉 인터넷 서비스 관리자' 선택
– 해당 관리자페이지 폴더에 오른쪽 클릭을 하고 등록정보 〉 디렉터리 보안 〉 IP 주소 및 도메인 이름 제한 〉 편집 버튼을 클릭
– 액세스 거부를 선택하고 추가 버튼을 클릭하여 관리자 호스트IP 또는 서브넷을 등록



2. 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 어용된 IP만 접근이 가능하도록 제어가 가능

Tomcat 서버설정 예

```
〈Host ...〉
〈Context path=" /KISAadm"  docBase=" /tomcat/webapps/ROOT/KISAadm" 〉
〈Valve className=" org.apache.catalina.valves.RemoteHostValve"
allow=" 192.168.1.2" /〉
〈/Context〉
〈/Host〉
```

※ 한국인터넷진흥원 홈페이지(http://www.kisa.or.kr) 〉 자료실 〉 관련법령·기술안내서 〉 기술안내서 가이드 〉 홈페이지 개발보안 안내서(p40), 홈페이지 취약점 진단제거 가이드(p67)

Key 3

주기적으로 홈페이지의 개인정보 노출여부를 점검하는 것이 좋습니다.

☞ 웹사이트 변경(통합, 개선, 복구 등)시 다음 사항을 점검 합니다.
- 웹 취약점 진단 및 시큐어 코딩 준수여부 점검 합니다.
- 회원 식별자를 개인정보로 사용하고 있는지 점검 합니다.
- 암호화 대상인 개인정보의 암호화 여부를 점검 합니다.
- 변경된 웹사이트는 외부에 공개하기 전에 개인정보 포함 여부를 점검 합니다.

☞ 주기적으로 외부 검색엔진에 개인정보가 수집되는지 점검 합니다.
- 검색엔진 고급검색 기능을 이용하여 개인정보를 주기적으로 점검 합니다.
  (검색단어 : “번호” , “주민” , “전화” , “여권” 등 활용)
- 디렉터리 리스팅 여부를 점검 합니다.
  ※ [참고 3] 구글 웹마스터 도구 사용법 참조

Key 4

게시글에 비공개 설정 기능이 있는 것이 좋습니다.

☞ 자주 묻는 질문(Q&A) 게시판과 1:1 상담 게시판을 분리하여 운영합니다.
- Q&A 게시판은 담당자가 관리하고 누구나 읽을 수 있도록 공개로 운영합니다.
- 1:1 상담 게시판은 작성자와 담당자만 읽을 수 있도록 비공개로 운영합니다.

※ 민원, 신청서 업로드 등 개인정보가 포함될 가능성이 많은 게시판은 비공개로 운영합니다.

☞ 개인정보가 포함된 경우, 즉시 삭제할 수 없을 때는 비공개로 전환합니다.

Key 5

게시글 작성 시 개인정보 노출주의에 대한 안내를 하는 것이 좋습니다.

☞ 홈페이지 이용자가 게시판을 이용 시 개인정보 노출예방에 대한 안내를 받을 수 있도록 글 작성 페이지에 안내글이나 팝업창을 제공 합니다.

용어 정의

이 안내서에서 사용하는 용어의 뜻은 다음과 같습니다.

용어	용어 정의
개인정보	살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말합니다. (개인정보 보호법 제2조)
개인정보 마스킹	개인정보 보호를 위해 주민등록번호, 의료보험번호, 여권번호, 운전면허번호 같은 개인정보의 일부분을 블라인드 처리하여 표시하는 방법을 말합니다.
개인정보 검색 솔루션	홈페이지 내에 존재하는 개인정보를 검색하여 개인정보의 위치를 확인해주는 솔루션을 말합니다.
개인정보 차단 솔루션	홈페이지 내에 게시글 등록 시 본문 내용 또는 첨부되는 파일 안에 주민등록번호, 휴대폰번호 등 개인정보가 포함되어 있는지 검사 후 차단하는 솔루션을 말합니다.
개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말합니다. (개인정보 보호법 제2조)
개인정보취급자	개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 자를 뜻합니다. (개인정보 보호법 제28조)
검색엔진 (Search Engine)	인터넷상의 웹 사이트에 있는 각종 정보를 검색해주는 기능을 제공하는 프로그램입니다. 검색 엔진은 크게 웹 사이트를 검색하여 해당 정보를 수집하는 로봇 에이전트와 수집된 자료가 저장되는 데이터베이스, 그 데이터베이스에서 자료를 검색하는 검색 프로그램으로 구성됩니다. 로봇 에이전트가 인터넷을 검색하여 수집한 정보들의 위치를 데이터베이스로 구축해 놓고, 이용자가 검색어를 입력하면 관련된 정보의 위치를 알려 줍니다.
공공기관	국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체와 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관을 말합니다.
디렉터리 (Directory)	디지털 자료 저장장치인 하드디스크에 저장된 파일들을 담고 있는 영역을 말하며, 디렉터리에는 그 속에 저장된 각각의 파일에 대한 이름과 크기, 위치 등이 기록되어 있습니다.
디렉터리 리스팅 취약점 (Directory Listing Vulnerability)	WEB이나 FTP 서비스의 취약한 설정으로 인해 서버의 디렉터리 및 파일에 열람 및 다운로드가 가능하게 되는 취약점입니다. 인터넷 이용자가 모든 디렉터리 및 파일 목록을 볼 수 있어 비공개 자료가 유출될 수 있습니다.

용어	용어 정의
보이스피싱 (Voice Phishing)	전화를 통해 불법적으로 개인 정보(주민등록번호, 신용카드번호, 은행계좌번호 등)를 빼내 범죄에 사용하는 신종 전화 사기 수법입니다. 음성(voice), 개인 정보(personal information) 및 낚시(fishing)를 합성한 신조어입니다. 기존의 피싱은 이메일을 통해 중요 정보를 입력하게 하는 소극적인 방법인 데 반해, 보이스피싱은 범행 대상자에게 전화를 걸어 송금을 요구하거나 개인 정보를 수집하는 적극적인 방법입니다.
세션 (Session)	네트워크 환경에서 사용자간 또는 컴퓨터 간 대화를 위한 논리적 연결을 의미합니다.
소스코드 (Source Code)	컴퓨터 프로그램을 만들기 위해 프로그래밍 언어로 기술한 글을 말합니다.
스팸 (Spam)	수신자의 의사와 관계없이 인터넷상의 다수 수신인에게 전자 우편(e-mail), 문자 메시지 등을 이용하여 무더기로 발송된 광고나 선전물을 의미합니다.
엑셀 (Excel)	미국 마이크로소프트(MS)사에 개발한 PC 용 수치관리 프로그램을 의미합니다. 많은 스프레드시트를 연결, 통합하여 다양한 도형과 차트 등 설명 자료를 작성하는 기능을 제공합니다.
웹 서버 (Web server)	웹 페이지가 들어 있는 파일을 이용자들에게 제공하는 프로그램입니다. 웹 사이트를 통해 서비스를 하려면 웹 서버 프로그램을 설치해야 합니다. 보편적인 웹 서버로는 아파치와 인터넷 인포메이션 서버, 엔터프라이즈 서버 등이 있습니다.
전용선	데이터 통신 등에서 각 장치들을 연결하는 회선으로 그 연결된 장치들만 사용할 수 있는 회선을 뜻합니다.
정규표현식	특정한 규칙을 가진 문자열의 집합을 표현하는 데 사용하는 형식 언어입니다. 정규표현식은 많은 텍스트 편집기와 프로그래밍 언어에서 문자열의 검색과 치환을 위해 사용하고 있습니다.
정보주체	처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말합니다. (개인정보 보호법 제2조)
개인정보의 처리	개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말합니다. (개인정보 보호법 제2조)
캐시 (Cache)	데이터 접근을 빠르게 할 수 있도록 미래의 요청에 대비해 데이터를 일시 저장해 두는 장소를 말합니다.

용어	용어 정의
크롤러 (수집기)	웹상의 다양한 정보를 자동으로 검색하고 색인하기 위해 검색엔진을 운영하는 사이트에서 사용하는 소프트웨어입니다. 사람들이 일일이 해당 사이트의 정보를 검색하는 것이 아니라 컴퓨터 프로그램의 미리 입력된 방식에 따라 끊임없이 새로운 웹 페이지를 찾아 종합하고, 찾아진 결과를 이용해 또 새로운 정보를 찾아 색인을 추가하는 작업을 반복 수행합니다. 스파이더(spider), 봇(bot), 또는 지능 에이전트라고도 합니다.
팝업창	특정 홈페이지가 어떠한 내용을 표시하기 위해 갑자기 생성되는 새 창을 말합니다.
포워드 (Forward)	클라이언트가 접속한 서버에서 다른 서버로 페이지 변경이 발생하는 경우를 말합니다.
포털사이트 (Portal Site)	인터넷의 출발점과 관문이 되는 사이트를 말하는데, 초기에는 인터넷을 항해하기 위한 출발점으로서의 역할만을 수행하였습니다. 그러나 현재는 특정 주제를 가지고 한 영역에서 전문정보를 제공하는 서비스나 필요한 모든 서비스를 한 사이트를 통해 제공받는 서비스를 의미합니다.
휴면 홈페이지	휴면 홈페이지는 장기간 동안 접속자가 없거나 관리가 이루어지지 않고 방치된 웹 사이트를 말합니다.
OLE (Object Linking and Embedding)	응용 프로그램 간 서로 호환이 되어 다른 응용 S/W에서 작성한 그림이나 표, 차트, 비디오 등과 같은 데이터의 정보를 연결시켜 주는 기능을 뜻합니다.
OWASP (The Open Web Application Security Project)	1984년 4월 안전한 웹 및 어플리케이션을 개발할 수 있도록 지원하기 위해 미국에서 비영리 단체로 출발한 전 세계 기업, 교육기관 및 개인이 만들어가는 오픈 소스 애플리케이션 보안 프로젝트입니다.
OWASP 10대 취약점	웹 애플리케이션 취약점 중에서 빈도가 높고, 보안상 악영향을 줄 수 있는 것들 10가지를 선정한 것입니다. ※ [참고 2] OWASP에서 발표한 10대 웹 애플리케이션 보안 취약점 참조
VPN (Virtual Private Network)	인터넷망을 전용선처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 기술로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용합니다.
URL (Uniform Resource Locator)	흔히 URL을 웹 사이트 주소로 알려져 있지만, 이는 웹 사이트 주소뿐만 아니라 컴퓨터 네트워크 상의 모든 자원을 나타낼 수 있습니다. URL은 주 컴퓨터의 이름과 주소, 파일이 있는 디렉터리 위치, 파일 이름으로 구성됩니다.

홈페이지 개인정보 노출방지 안내서

참고 1 홈페이지 개인정보 유출 시 신고절차

개인정보 처리자는 정보주체의 개인정보가 유출된 경우에 정보주체에게 지체 없이 통지하고 조치결과를 관계 중앙행정기관(행정자치부장관, 방송통신위원회) 또는 한국인터넷진흥원에 지체 없이 신고하여야 합니다.

다만, 오프라인 사업자의 경우에는 유출된 개인정보가 1만 명 이상인 경우에 행정자치부장관 또는 한국인터넷진흥원에 신고하면 됩니다.

[참고] 개인정보 보호법에서 '개인정보 유출 통지 및 신고' 처리에 대한 관련 법령은 다음과 같습니다.

관련 법령

[개인정보 보호법] 제34조 제3항(개인정보 유출 통지 등)

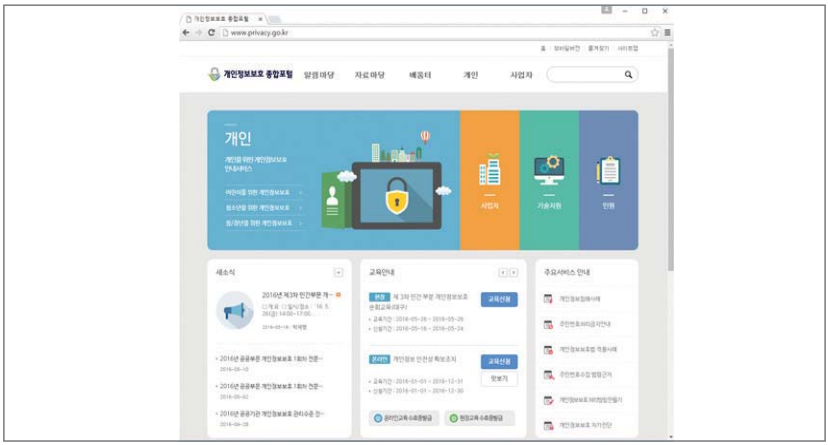
③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정자치부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

[개인정보 보호법 시행령] 제39조제1항(개인정보 유출 신고의 범위 및 기관)

① 법 제34조제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 1만 명 이상의 정보주체에 관한 개인정보를 말한다.

개인정보보호 종합포털을 통해 한국인터넷진흥원으로 온라인 신고하는 절차는 다음과 같습니다.

☑ 1단계 (개인정보보호 종합포털(www.privacy.go.kr)에 접속)

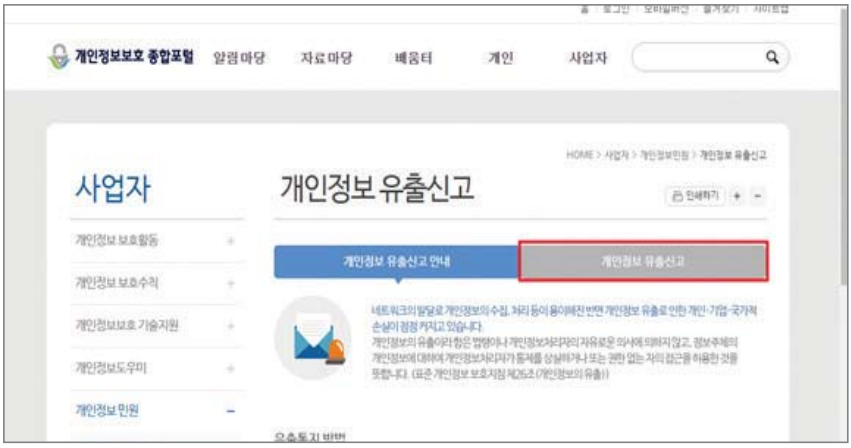


[그림 52] 개인정보보호 종합포털 화면

☑ 2단계 (사업자 메뉴 > 개인정보 민원 클릭)

[그림 53] 개인정보 민원 메뉴선택

3단계 (화면 우측 상단의 "개인정보 유출신고" 선택)



[그림 54] 개인정보 유출신고 선택

4단계 (웹 페이지 메시지 확인 후 "확인" 선택)

[그림 55] 개인정보 유출신고 메시지 확인

5단계 (개인정보 유출신고 작성)

[그림 56] 개인정보 유출신고 화면

[참고] 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 '개인정보 유출 통지 및 신고' 처리에 대한 관련 법령은 다음과 같습니다.

☑ 관련 법령

[정보통신망 이용촉진 및 정보보호 등에 관한 법률] 제27조의3 제1항(개인정보 누출등의 통지·신고)

① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등" 이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 〈개정 2014.5.28.〉

[정보통신망 이용촉진 및 정보보호 등에 관한 법률] 제27조의3 제1항(개인정보 유출등의 통지·신고)

① 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등" 이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 〈개정 2014.5.28., 2016.3.22.〉[본조신설 2012.2.17.] [제목개정 2016.3.22.] [시행일 : 2016.9.23.] 제27조의3

※ 2016년 9월 23일 이후로 제27조의3 제1항(개인정보 누출등의 통지·신고)가 제27조의3 제1항(개인정보 유출등의 통지·신고)로 변경됩니다.

[정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령] 제39조제1항(개인정보 누출 등의 통지·신고)

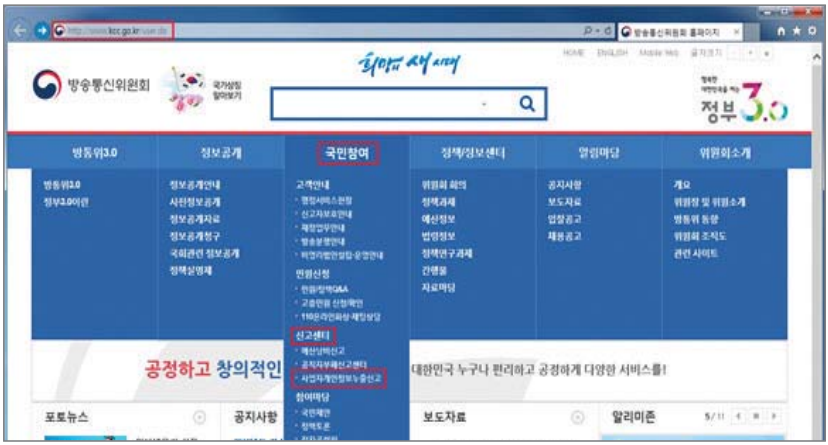
① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등" 이라 한다)의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.

개인정보보호 포털을 통해 방송통신위원회로 유출신고 하는 방법은 서면 신고와 온라인 신고로 구분되어 있습니다.

☑ 1단계 (방송통신위원회(www.kcc.go.kr)에 접속)

[그림 57] 방송통신위원회 홈페이지 화면

2단계 (국민참여 메뉴 > 신고센터 클릭 > 사업자 개인정보 누출신고 클릭)



[그림 58] 사업자 개인정보 누출신고 메뉴선택

3단계 (개인정보보호 포털(www.i-privacy.kr)로 이동)

[그림 59] 개인정보보호 포털 화면

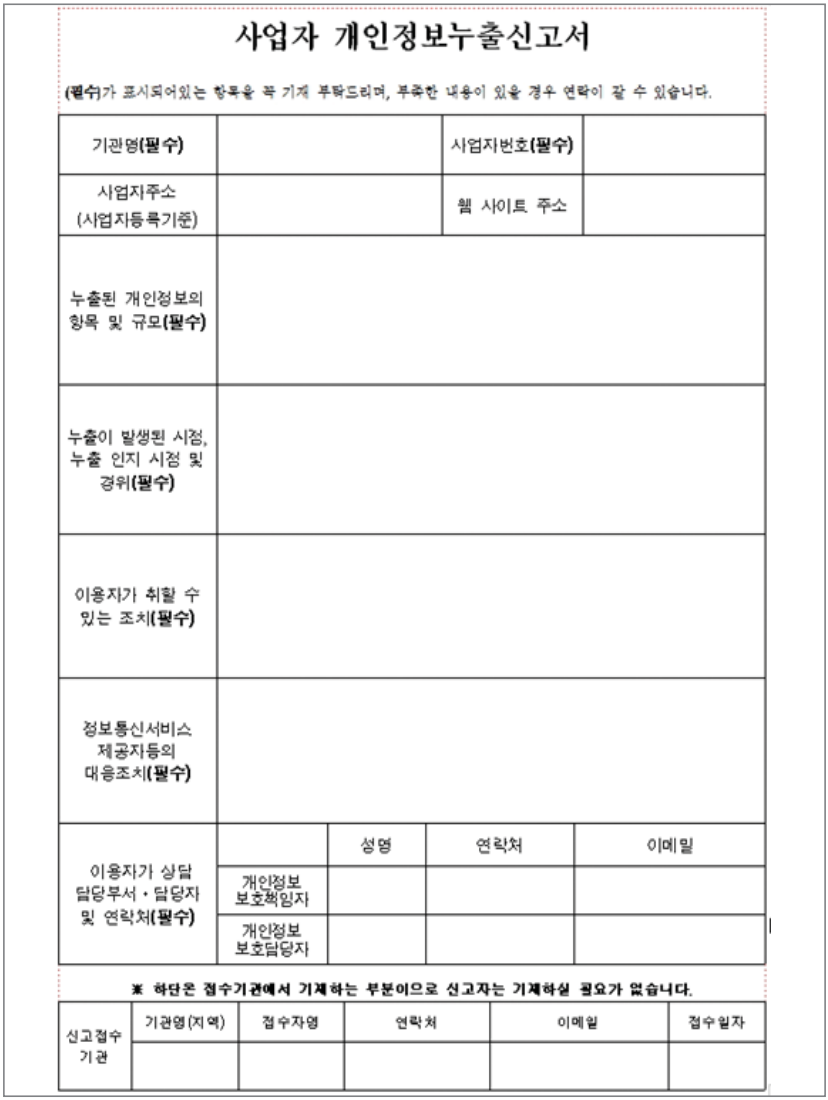
4단계 (개인정보 신고 메뉴 > 개인정보 누출신고 클릭)

[그림 60] 개인정보 누출신고 메뉴선택

5단계 [서면신고]의 경우 ('개인정보 누출신고 다운로드'를 클릭하여 양식 다운로드)

[그림 61] 개인정보 누출신고서 다운로드 선택

6단계 [서면신고]의 경우 (다운로드 받은 '사업자_개인정보 누출신고서'에 신고내용을 작성)



사업자 개인정보누출신고서

(필수)가 표시되어있는 항목을 꼭 기재 부탁드리며, 부족한 내용이 있을 경우 연락이 갈 수 있습니다.

기관명(필수)		사업자번호(필수)	
사업자주소 (사업자등록기준)		웹 사이트 주소	
누출된 개인정보의 항목 및 규모(필수)			
누출이 발생된 시점, 누출 인지 시점 및 경위(필수)			
이용자가 취할 수 있는 조치(필수)			
정보통신서비스 제공자등의 대응조치(필수)			

이용자가 상담 담당부서·담당자 및 연락처(필수)		성명	연락처	이메일
	개인정보 보호책임자			
	개인정보 보호담당자			

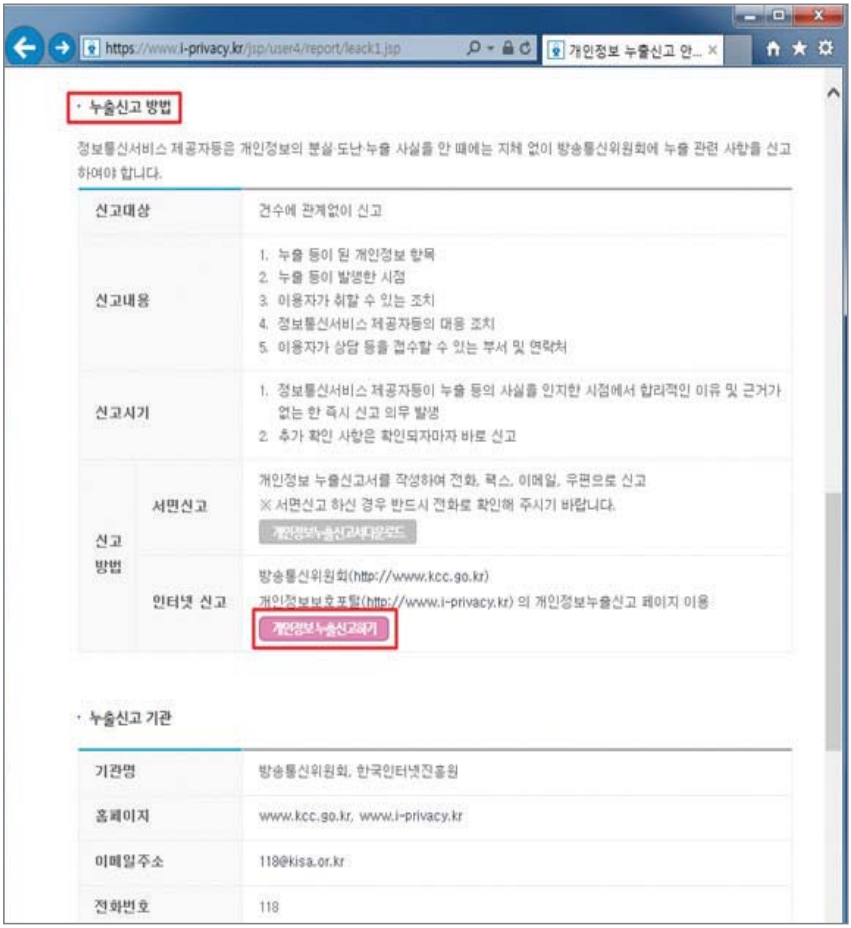
※ 하단은 접수기관에서 기재하는 부분이므로 신고자는 기재하실 필요가 없습니다.

신고접수 기관	기관명(지역)	접수자명	연락처	이메일	접수일자

[그림 62] 사업자 개인정보 누출신고서 양식

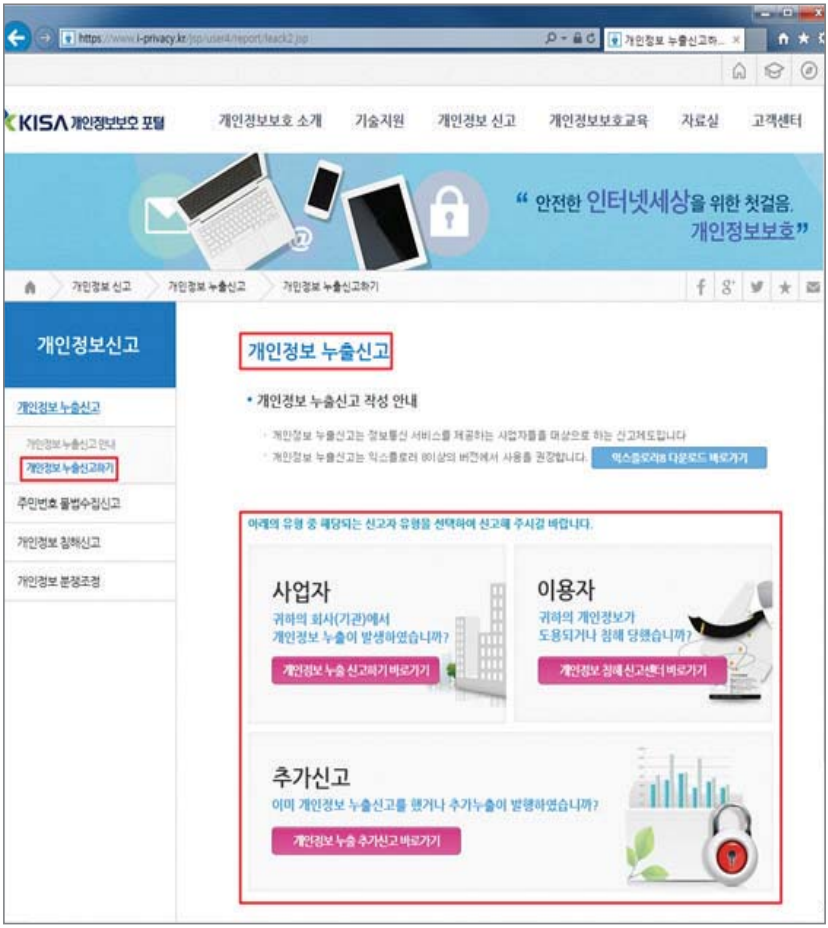
※ 서면신고의 경우 누출신고서를 작성하여 전화, 팩스, 이메일, 우편으로 신고하시면 됩니다.
연락처는 [그림 61]의 누출신고 기관 연락처를 참고하시면 됩니다.

☑ 5단계 [인터넷 신고]의 경우 ('개인정보 누출신고하기'를 클릭)



[그림 63] 개인정보 누출신고하기 클릭

6단계 [인터넷 신고]의 경우 (3가지 유형 중 해당되는 신고자 유형을 클릭 후 신고)



[그림 64] 신고자 유형 선택

참고 2 OWASP[1] 에서 발표한 10대 웹 애플리케이션 보안 취약점

[표 8] 2013년 OWASP 10대 보안 취약점

항목	내용
A1. 인젝션 (Injection)	이용자가 입력한 데이터가 명령어나 질의문의 일부분으로 웹 서버의 데이터베이스나 백엔드 시스템의 인터프리터에 연결되어 명령어 실행 및 데이터 변경이 실행되는 취약점
A2. 취약한 인증 및 세션관리 (Broken Authentication and Session Management)	계정에 대한 증명과 세션토큰이 적절히 보호되지 못함으로 인해 패스워드나 키, 세션쿠키, 다른 토큰 등을 악용하여 인증 메커니즘을 무력화 시키거나 다른 이용자의 아이디를 추측할 수 있는 취약점
A3. 크로스사이트 스크립트(XSS) (Cross-Site Scription)	악의적인 공격자가 타인의 브라우저 내에서 스크립트를 실행하도록 허용함으로써 타인의 세션을 가로채거나 웹 사이트를 손상하거나 웜을 삽입하는 등을 가능하게 하는 취약점
A4. 불안전한 직접객체 참조 (Insecure Direct Object References)	파일, 디렉터리, 데이터베이스 기록, 키 등의 내부 구현 객체에 대한 참조 정보를 URL 또는 폼 파라미터로 노출시켜서 악의적인 공격자가 이를 조작하여 인증절차 없이 다른 객체에 접속할 수 있도록 하는 취약점
A5. 보안상 잘못된 구성 (Security Misconfiguration)	어플리케이션, 프레임워크, 어플리케이션 서버, 웹 서버, 데이터베이스 서버와 플랫폼에 대한 적절한 보안 구성에 대한 정의 및 적용 여부, 어플리케이션 코드 라이브러리를 포함한 소프트웨어의 최신 업데이트 유지
A6. 민감한 데이터 노출 (Sensitive Data Exposure)	카드번호 같은 민감한 데이터를 암호화하지 않거나 데이터 전송 시 암호화 등을 거치지 않아 악의적인 공격자에 의해 민감 데이터가 노출되는 취약점
A7. 기능접근제어누락 (Missing Function Level Access Control)	어플리케이션은 각 기능에 대한 접근 시 동일한 접근제어검사 수행이 요구됨. 접근제어검사가 적절하지 않을 경우 악의적인 공격자는 비인가된 기능에 접근하기 위해 정상적인 요청을 변조할 가능성이 있음
A8. 크로스사이트 변조요청(CSRF) (Cross-Site Request Forgery)	로그온을 한 이용자의 브라우저가 사전에 승인된 요청을 웹 서버에 보내도록 함으로써 악의적인 공격자가 의도하는 공격을 수행하도록 하는 취약점
A9. 취약점이 있는 컴포넌트 사용 (Using Known Vulnerable Components)	슈퍼유저권한으로 운영되는 취약한 컴포넌트(라이브러리, 프레임워크 및 기타 소프트웨어 모듈)로 인해 데이터 유실 및 서버 권한 획득과 같은 취약성 존재
A10. 검증되지 않은 리다이렉트와 포워드(Unvalidated Redirects and Forwards)	웹 어플리케이션은 목적페이지를 결정하기 위해 신뢰되지 않은 데이터를 사용하기 때문에 적절한 확인이 없다면, 공격자는 피싱사이트나 악의적인 사이트로 리다이렉트 유도 및 권한없는 페이지에 포워드를 시도함

1) OWASP(Open Web Application Security Project)

1984년 4월 안전한 웹 및 응용을 개발할 수 있도록 지원하기 위해 미국에서 비영리 단체로 출발한 전 세계 기업, 교육기관 및 개인이 만들어가는 오픈 소스 애플리케이션 보안 프로젝트

참고 3 구글 웹마스터 도구 사용법

1. 서치 콘솔(Search Console) 도움말

구글(Google)의 저장된 페이지에서 개인정보가 노출될 경우, 구글에서 제공하고 있는 웹마스터 도구를 이용하여 검색엔진의 "저장된 페이지" (캐시)를 삭제요청 할 수 있습니다. 웹마스터 도구 삭제 요청 절차를 자세히 살펴보도록 하겠습니다.

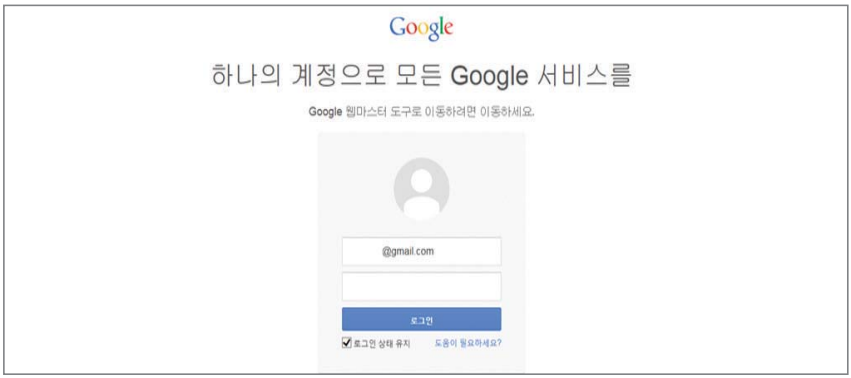
구글(Google) 웹마스터 도구란 이용자 페이지의 게재빈도와 관련된 자세한 보고서를 제공해주고 홈페이지에 대한 정보를 확인할 수 있게 해주는 도구입니다.

[그림 65] 구글 웹마스터 도구 도움말 접속 화면

참조 : 구글 웹마스터 도구 도움말 :
https://support.google.com/webmasters/?hl=ko#topic=3309469

가. 구글 웹마스터 도구에서 홈페이지의 소유권 확인 방법

1단계 (로그인)



[그림 66] 구글 웹마스터 도구 로그인

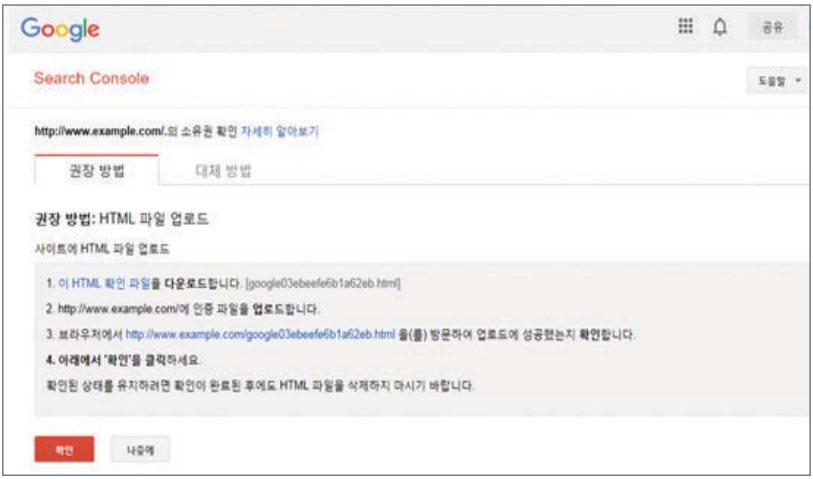
2단계 (사이트 추가)

[그림 67] 사이트 추가 클릭

3단계 (사이트 URL 추가)

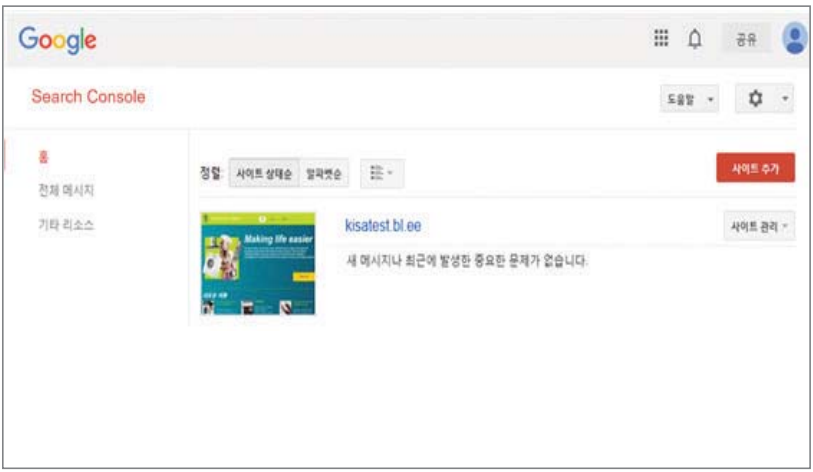
[그림 68] 사이트 URL 입력

4단계 (사이트 소유권 인증)



[그림 69] HTML 파일 업로드

5단계 (사이트 추가 완료)



[그림 70] 사이트 등록 화면

구글 웹마스터 도구에 사이트 등록이 완료되었습니다. 이제 구글 검색엔진에서 검색된 결과를 삭제할 수 있는 방법을 알아보도록 하겠습니다.

사이트에 노출된 개인정보를 삭제하려면 홈페이지에 노출된 개인정보를 삭제한 후 웹마스터 도구를 이용해 캐시에 노출된 페이지를 삭제요청 해야 합니다.

[표 9] 웹마스터 도구를 이용한 삭제방법들의 차이점

삭제방법	차이점	비고
Fetch As Google	검색엔진에 홈페이지 재 수집 요청 기능	사이트소유권확인 필요
	(예시) 홈페이지의 개인정보를 삭제 후 홈페이지 정보를 재수집하도록 요청할 경우 (예시) 다수 페이지에 개인정보가 노출된 경우 (예시) 내부 업무용 게시판, FTP 등에서 개인정보가 노출된 경우	
URL 삭제	긴급하게 사이트를 구글 검색결과에서 삭제하는 기능 (주의) 글 검색결과에서 일시적으로 제외하는 방법이므로 홈페이지조치 미흡 시 재 노출 될 가능성이 있음	
	(예시) 다수 페이지에 개인정보가 노출된 경우	
오래된 콘텐츠 삭제	오래된 캐시 정보 삭제 기능 (참고) 홈페이지가 삭제된 경우, 관리자 아니더라도 삭제 요청 가능	사이트 소유권 확인 필요 없음
	(예시) 홈페이지에서는 삭제되었지만, 캐시에 개인정보가 노출된 경우	

나. 웹마스터 도구 이용 시 주의 사항

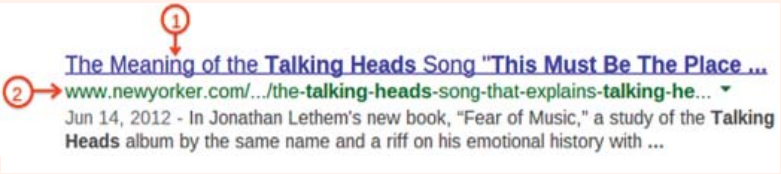
구글 웹마스터 도구를 이용하여 삭제요청을 할 경우, URL을 정확히 입력해야 합니다. URL은 대문자와 소문자를 구분해야 하며, 검색결과에 표시되는 정확한 URL을 입력해야 합니다. 정확한 URL을 확인하는 방법에 대해 알아보도록 하겠습니다.

페이지 URL 찾기

URL 삭제 또는 순위 강등을 요청할 때에는 검색결과에 표시되는 정확한 URL을 입력해야 합니다. URL의 작은 차이(예: www.example.com/dragon과 www.example.com/Dragon)가 중요하지 않게 보일 수 있지만, 예로든 두 URL은 실제로 다른 URL이며 일부 서버에서는 다른 콘텐츠로 연결될 수 있습니다. 검색결과에 표시되는 정확한 URL을 입력해야만 Google에서 원하는 콘텐츠를 삭제하거나 콘텐츠의 순위를 낮출 수 있습니다. 다음은 정확한 URL을 찾기 위한 몇 가지 도움말입니다.

줄임표

검색결과 페이지의 녹색 URL에 줄임표(...)가 포함되어 있으면 대개 화면 표시를 위해 URL을 짧게 표시한 것입니다.



줄임표가 있는 URL은 복사하여 붙여 넣지 마십시요. 대신 검색결과의 제목(위의 이미지에서 1로 표시)을 클릭합니다. 페이지가 열리면 브라우저의 주소 표시줄에서 URL을 복사합니다.

URL을 찾는 또 다른 방법은 검색결과의 링크를 마우스 오른쪽 버튼으로 클릭한 다음 URL을 복사하는 것입니다. 복사한 URL을 URL 삭제 도구 또는 사이트링크 순위 강등 도구에 붙여넣으면 www.google.com으로 시작하는 매우 긴 URL이 표시됩니다. Google에서 올바른 URL을 식별할 수 있으므로 URL이 길어도 걱정하지 마십시요.

대문자 표시

URL 삭제 도구 및 사이트링크 순위 강등 도구는 대소문자를 구분합니다. 즉, www.example.com/nunchuckskills를 입력할 경우 www.example.com/NunchuckSkills는 삭제되거나 순위가 낮아지지 않으며 그 반대의 경우도 마찬가지입니다. 따라서 Google 검색결과에 나타나는 URL과 동일한 대소문자 조합의 URL을 입력해야 합니다. 다시 한 번 강조하지만, 페이지를 열고 주소 표시줄에서 URL을 복사하는 것이 정확한 URL을 얻는 가장 확실한 방법입니다.

이미지

이미지 삭제 요청을 제출하려는 경우 올바른 URL을 찾는 방법은 다음과 같습니다.
1. 이미지 검색결과에 있는 이미지를 클릭합니다.
2. 원본 이미지 보기 또는 전체 크기를 마우스 오른쪽 버튼으로 클릭하고 링크 주소를 복사합니다.
3. URL 삭제 도구에서 사용할 수 있도록 URL을 파일 또는 문서에 붙여넣습니다.

여러 URL

동일한 콘텐츠가 여러 URL에 나오는 것은 일반적이며 포럼 또는 대화목록 기반 홈페이지에서는 이런 경우가 더욱 많습니다. 예를 들면 다음과 같습니다.

http://www.example.com/forum/thread/123
http://www.example.com/forum/post/456
http://www.example.com/forum/thread/123?post=456
http://www.example.com/forum/thread/123?post=456&sessionid=12837460

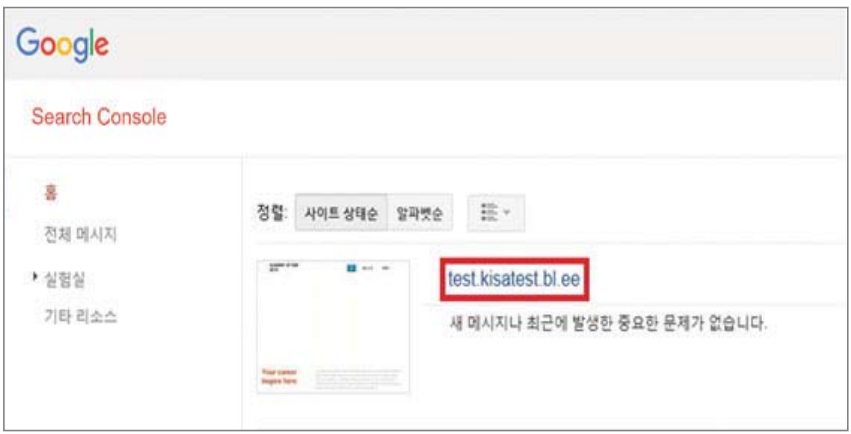
URL 하나의 삭제 또는 순위 강등 요청을 완료한 경우에도 삭제하려는 콘텐츠가 다른 URL로 Google 검색결과에 나타날 수 있습니다. 이 경우에는 이 콘텐츠를 표시하는 각 URL의 삭제 요청을 추가로 제출하면 됩니다.

삭제 요청의 상태가 '삭제됨'으로 표시되지만 검색결과에 삭제 요청한 콘텐츠가 계속 표시되는 경우 검색결과에 나타나는 URL이 삭제를 위해 제출한 URL과 대소문자를 포함하여 정확하게 동일한지 확인해 보세요. 동일하지 않은 경우에는 현재 검색결과에 나타나는 URL의 삭제를 추가로 요청해야 합니다.

[출처] 웹마스터 도구 사용 도움말(https://support.google.com/webmasters/answer/63758?hl=ko)

다. Fetch As Google 이용 방법(사이트 관리자일 경우에만 유효)

1단계 (사이트 선택)



[그림 71] 추가된 도메인 클릭

2단계 (사이트 크롤링 요청)

[그림 72] 'Fetch As Google' 클릭

3단계 (사이트 주소 입력)

[그림 73] 사이트 주소 입력 후 '가져오기' 클릭

4단계 (사이트 재수집 요청)

[그림 74] '색인에 제출' 클릭

5단계 (재수집 범위 선택)

[그림 75] '이 URL 및 직접 연결되는 링크 크롤링' 을 선택 후 확인 클릭

6단계 (사이트 재수집 요청 후 반영까지 일주일 정도 소요)

[그림 76] 삭제 신청 및 확인

라. URL 삭제 이용 방법(사이트 관리자일 경우에만 유효)

구글 검색 결과에서 'URL 제거' 기능은 특정 사이트나 URL을 긴급 삭제하는 기능으로 홈페이지가 삭제되지 않더라도 구글 검색결과에서 임시 삭제됩니다. (임시적인 조치로 검색결과에서는 일정기간 동안만 보이지 않음)

(주의) 삭제 조치가 미흡할 경우 노출될 가능성이 있으므로 홈페이지의 노출된 개인정보 삭제 후 'URL 제거' 기능을 이용해야 합니다.

☑ 1단계 (사이트 선택)

[그림 77] 삭제를 원하는 사이트 선택 클릭

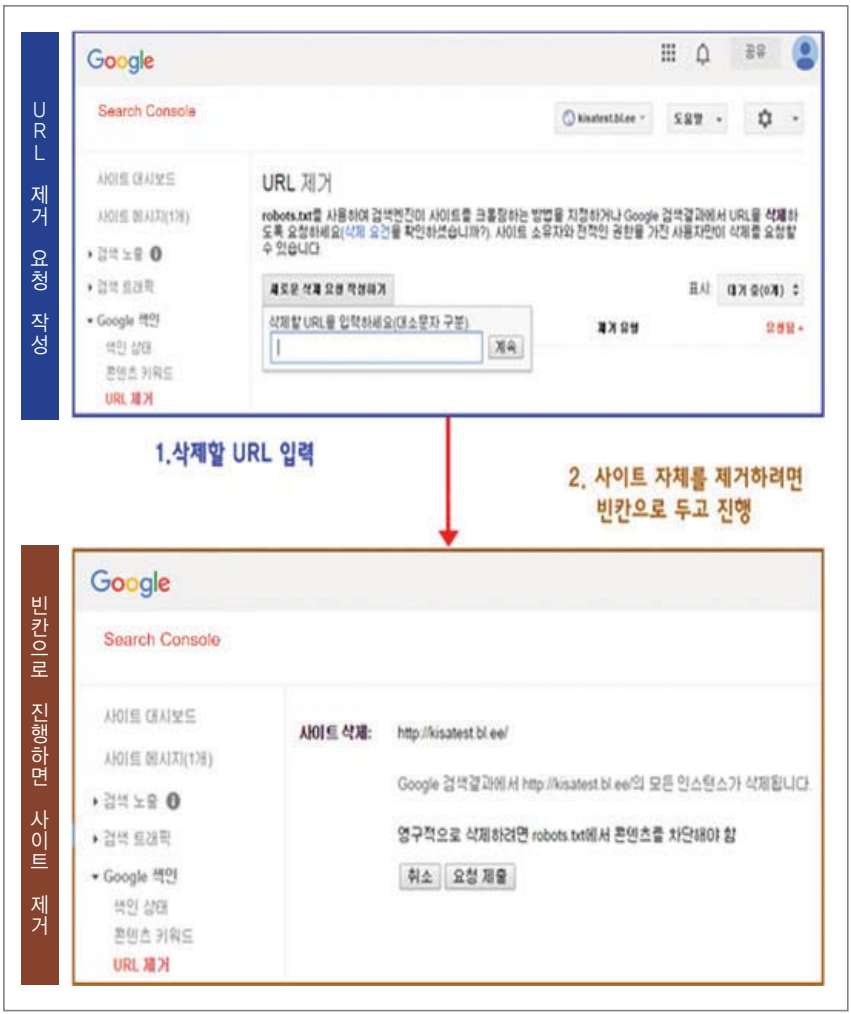
☑ 2단계 (URL 제거 도구 선택)

[그림 78] 'URL 제거' 선택 클릭

☑ 3단계 (삭제 요청)

[그림 79] '새로운 삭제 요청 작성하기' 클릭

4단계 (삭제할 URL 입력, 사이트 자체를 제거하려면 빈칸으로 두고 진행)



[그림 80] 삭제할 URL 입력 후 요청 제출 클릭

5단계 (삭제 사유 선택 후 반영까지 일주일 정도 소요)

[그림 81] 캐시 URL 삭제 이유 선택

[표 10] 캐시 URL을 삭제하고자 하는 이유에 대한 설명

항목	설명
검색결과 및 캐시에서 페이지 삭제	내 사이트 URL에 대한 검색결과 및 캐시페이지를 전부 삭제할 때 신청합니다.
캐시에서만페이지 삭제	사이트에서 페이지를 업데이트하면, 다음에 크롤링 할 때 Google은 캐시된 버전을 비롯하여 색인을 업데이트합니다. 업데이트가 완료될 때까지는 원본 콘텐츠가 캐시에 포함되어 검색결과에 해당 콘텐츠가 표시될 수 있습니다. 오래된 콘텐츠의 삭제를 요청할 수 있으며 이 경우 페이지 미리보기도 삭제됩니다.
디렉터리 삭제	디렉터리나 사이트를 영구적으로 삭제하려면 'robots.txt' 를 사용하여 크롤러가 디렉터리에 액세스하지 못하게 차단하고, 사이트를 삭제하는 경우에는 전체 사이트에 대한 액세스를 차단해야 합니다. 이 작업은 디렉터리 삭제를 요청하기 전이나 요청한 후 곧바로 수행하는 것이 좋습니다. 그렇지 않을 경우, 콘텐츠가 나중에 검색결과에 다시 표시될 수 있습니다.

참고사항

[구글 웹마스터 도구]를 통해 구글 검색결과나 캐시 페이지 삭제요청은 가능하나, 요청을 한다고 해서 반드시 삭제되는 것은 아니며, 구글의 판단에 따라 요청이 거부될 수도 있습니다.

구글의 개인정보 보호정책은 주민등록번호와 같은 국가 발급 번호에 대한 개인정보가 노출 되었을 경우만 삭제 혹은 마스킹(* 처리)이 가능하며, 주민등록번호 이외의 정보에 대해서는 삭제가 되지 않을 수 있습니다.

※ 참조 : 구글 웹마스터도구 FAQ(http://support.google.com/webmasters/answer/1050724?hl=ko)

참고 4 로봇배제표준

가. 개요

로봇배제표준이란 검색로봇의 접근범위를 제한하는 규약으로, 웹 서버에 설정파일(robots.txt)을 만들어 사용합니다.

검색로봇이란 검색엔진이 홈페이지 정보를 수집하기 위해 인터넷을 돌아다니는 소프트웨어를 말합니다.

나. 로봇배제표준에 대한 이해

1) 로봇배제표준은 단순 규약입니다.
로봇배제표준은 국제 표준이 아닌 규약이므로 검색로봇이 반드시 준수하지 않을 수 있습니다.

2) 로봇배제표준은 이용자의 접근과 무관합니다.
로봇배제표준은 검색로봇의 접근범위를 제한하므로, 홈페이지를 이용하는 사람에 대한 접근을 제한하지 않습니다.

3) 로봇배제표준 설정은 누구나 볼 수 있습니다.
robots.txt 파일은 누구나 읽을 수 있으므로 공개된 페이지에 적용하여야 하며, 민감정보(디렉터리, 관리자페이지 정보 등)가 포함되지 않도록 관리자의 주의가 필요합니다.

※ 공개된 페이지 : 글쓰기가 가능하지만 로그인을 하지 않는 게시판 등

4) 로봇배제표준은 개인정보 노출 예방을 위한 임시도구입니다.
보다 안전하게 개인정보 노출을 예방하기 위해서는 기관 담당자가 홈페이지에 개인정보가 게시되지 않도록 주기적인 취약점검, 게시판 비밀번호 설정 및 개인정보 검색/유출차단 시스템 도입 등의 조치를 해야만 합니다.

개인정보 노출 예방을 위해 개인정보 검색/유출차단 솔루션의 도입을 권고하며, 로봇배제표준은 솔루션 도입이 어려운 기관에서 공개된 개인정보가 외부 검색엔진에 검색되는 것을 방지하기 위한 임시도구로 활용하도록 해야 합니다.

다. 로봇배제표준 적용 시 유의점

로봇배제표준은 적용범위에 따라 검색엔진에서 홈페이지 정보가 검색되지 않을 수 있으므로 주의해야 하며, 홈페이지의 용도 및 개인정보 노출방지/차단 솔루션 운영여부 등을 고려하여 기관담당자의 판단에 따라 사용여부를 결정해야 합니다.

라. 로봇배제표준 설정방법

robots.txt 파일의 내용은 크게 2가지로 나뉘는데, 로봇의 이름을 적는 부분(User-agent)과 방문의 허용 여부를 적는 디렉터리 부분(Allow 및 Disallow)으로 구분됩니다.

로봇배제표준 문법을 참고하여 robots.txt 작성한 후 웹 서버의 각 도메인별 최상위 주소에 저장하면 됩니다.

예시) http://www.example.or.kr/robots.txt
※ robots.txt를 다른 디렉터리에 놓는 경우 효력이 없으므로 주의해야 합니다.

1) robots.txt 문법 설명

· (전면허용) 모든 로봇의 접근을 "전면허용" 하는 경우
  User-agent: *
  Allow: /

· (전면차단) 모든 로봇의 접근을 "전면차단" 하는 경우
  User-agent: *
  Disallow: /

· (부분차단) 모든 로봇의 특정 디렉터리 및 파일 접근을 "부분차단" 하는 경우
  User-agent: *
  Disallow: /directory_or_url

· (특정파일) 모든 로봇이 xls 파일에 접근을 차단하는 경우
  User-agent: *
  Disallow: /*.xls

· (특정파일) 특정 로봇의 접근만 "전면허용" 하는 경우 User-agent: 검색로봇명
  Allow:User-agent: *
  Disallow: /

[표 11] robots.txt 작성 시 유의사항

유의사항	잘못된 예시	잘된 예시
대소문자 구분	User-Agent: * disallow: /directory_or_url ※ User-agent의 A가 대문자 ※ Disallow의 d가 소문자	User-agent: *Disallow: /directory_or_url
띄어쓰기	User-agent : * Disallow:/directory_or_url ※ User-agent와 콜론(:)이 떨어짐 ※ Disallow 이후 콜론(:)과 슬래시(/)가 붙음	User-agent: *Disallow: /directory_or_url
줄바꾸기	User-agent: 검색로봇명1 Disallow: /directory_or_url User-agent: 검색로봇명2 Disallow: /directory_or_url ※ 다중 검색로봇을 지정 시, 한 줄을 띄우지 않음	User-agent: 검색로봇명1 Disallow: /directory_or_url User-agent: 검색로봇명2 Disallow: /directory_or_url
설정 파일이름	robot.txt ※ 설정파일 이름은 “robots.txt” 로 해야함	robots.txt
설정파일 적용 위치	examle.or.kr/sub_directory/robots.txt ※ 파일 위치는 홈페이지의 최상위 디렉터리(/)이어야 함	example.or.kr/robots.txt
적용대상	www.example.or.kr ※ 기관 홈페이지가 복수 개인 경우 (각각 도메인이 다른 경우) 모두 개별적으로 적용해야 함	http://www.example.or.kr http://example.or.kr https://www.example.or.kr http://edu.example.or.kr http://media.example.or.kr

[표 12] 검색엔진별 검색로봇 리스트

검색엔진	검색로봇
다음	Daumoa
구글	Googlebot
야후	Yahoo! Slurp
네이버	Naverbot
Bing	Bingbot
Microsoft	Msnbot
네이트	Natebot

참고 5 고유식별정보 정규표현식

개인정보를 검사하는 정규표현식(패턴)

▶ 주민등록번호
([01][0-9]{5}[[:space:],~-]+[1-4][0-9]{6}|[2-9][0-9]{5}[[:space:],~-]+[1-2][0-9]{6})

▶ 여권번호
[a-zA-Z]{2}[-~.[:space:]][0-9]{7}

▶ 운전면허번호
[0-9]{2}[-~.[:space:]][0-9]{6}[-~.[:space:]][0-9]{2}

▶ 핸드폰번호
01[016789][-~.[:space:]][0-9]{3,4}[-~.[:space:]][0-9]{4}

▶ 신용카드번호
[34569][0-9]{3}[-~.[:space:]][0-9]{4}[-~.[:space:]][0-9]{4}[-~.[:space:]][0-9]{4}

▶ 건강보험번호
[1257][-~.[:space:]][0-9]{10}

▶ 계좌번호
([0-9]{2}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{6}|[0-9]{3}[-~.[:space:]]([0-9]{5,6}[-~.[:space:]][0-9]{3}|[0-9]{6}[-~.[:space:]][0-9]{5}|[0-9]{2,3}[-~.[:space:]][0-9]{6}|[0-9]{2}[-~.[:space:]][0-9]{7}|[0-9]{2}[-~.[:space:]][0-9]{4,6}[-~.[:space:]][0-9]|[0-9]{5}[-~.[:space:]][0-9]{3}[-~.[:space:]][0-9]{2}|[0-9]{2}[-~.[:space:]][0-9]{5}[-~.[:space:]][0-9]{3}|[0-9]{4}[-~.[:space:]][0-9]{4}[-~.[:space:]][0-9]{3}|[0-9]{6}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{3}|[0-9]{2}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{7})|[0-9]{4}[-~.[:space:]]([0-9]{3}[-~.[:space:]][0-9]{6}|[0-9]{2}[-~.[:space:]][0-9]{6}[-~.[:space:]][0-9])|[0-9]{5}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{6}|[0-9]{6}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{5,6}).


행정자치부
한국인터넷진흥원