



홈페이지 개인정보 노출방지 안내서

2016.06



행정자치부



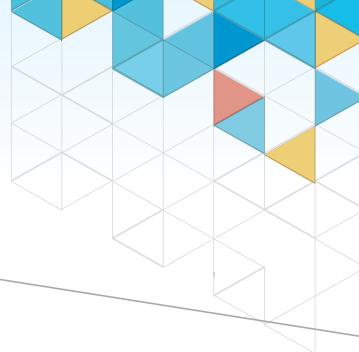
한국인터넷진흥원

제 · 개정 이력

본 “홈페이지 개인정보 노출방지 안내서”는 ‘08년 2월 제정 이후 5차 개정판입니다.

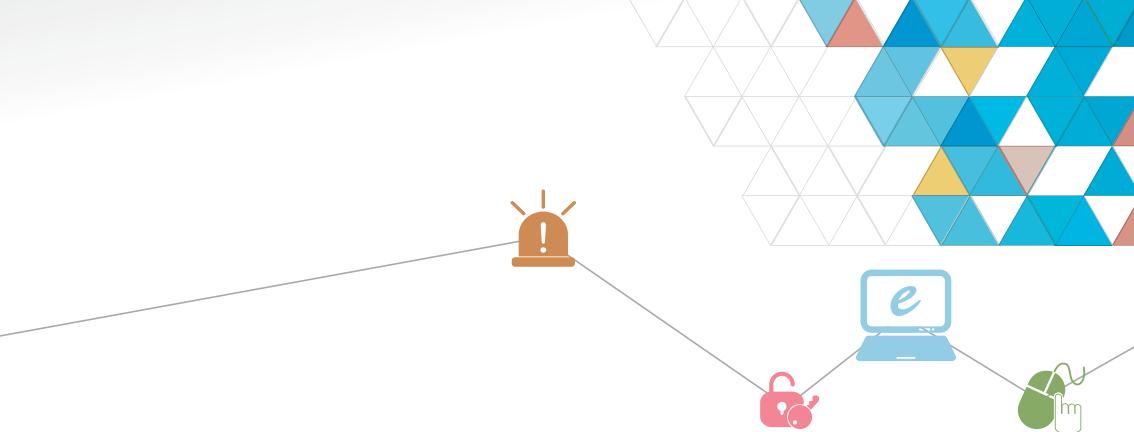
구분	일자	비고
제정	2008.02	
1차 개정	2009.02	
2차 개정	2011.05	
3차 개정	2012.08	
4차 개정	2014.12	
5차 개정	2016.06	

- 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 돋기 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.



I CONTENTS

① 개요	07
1. 개인정보란?	08
2. 개인정보 노출이란?	10
3. 개인정보 노출 시 어떤 위험이 있나요?	11
② 개인정보 노출 원인별 사례분석	13
1. 홈페이지 설계 및 관리 미흡으로 인한 노출	20
2. 첨부파일에 의한 노출	25
3. 게시글에 의한 노출	38
③ 개인정보 노출 시 조치 방법	41
1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법 ..	42
2. 첨부파일이 포함된 게시글 노출 시 조치 방법	53
3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법	55
4. 검색엔진에 저장된 페이지 삭제 방법 공통사항	56



④ 개인정보 노출 사전에 예방하세요 67

- 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 71

- >>> 참고 1 홈페이지 개인정보 유출 시 신고절차 76
- >>> 참고 2 OWASP에서 발표한 10대 웹 애플리케이션 보안 취약점 86
- >>> 참고 3 구글 웹마스터 도구 사용법 87
- >>> 참고 4 로봇배제표준 98
- >>> 참고 5 고유식별정보 정규표현식 101



홈페이지 개인정보 노출방지 안내서

I 개요

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





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.

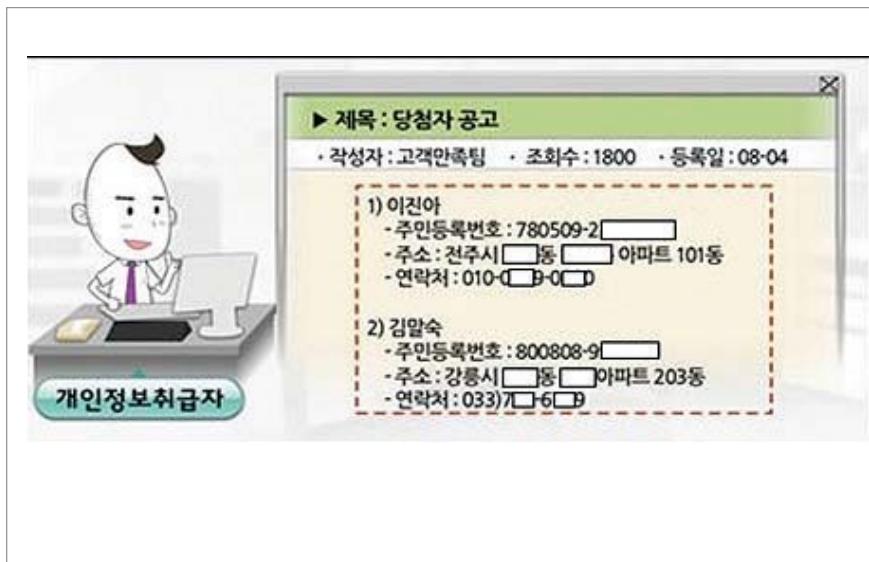


[표 1] 개인정보의 유형(예)

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, 기술자격증 및 전문 면허증, 학교성적, 동아리활동, 상벌사항, 이수한 훈련 프로그램,	병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유자량, 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	대출잔액 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. 민감 정보와 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)



홈페이지 개인정보 노출방지 안내서

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.

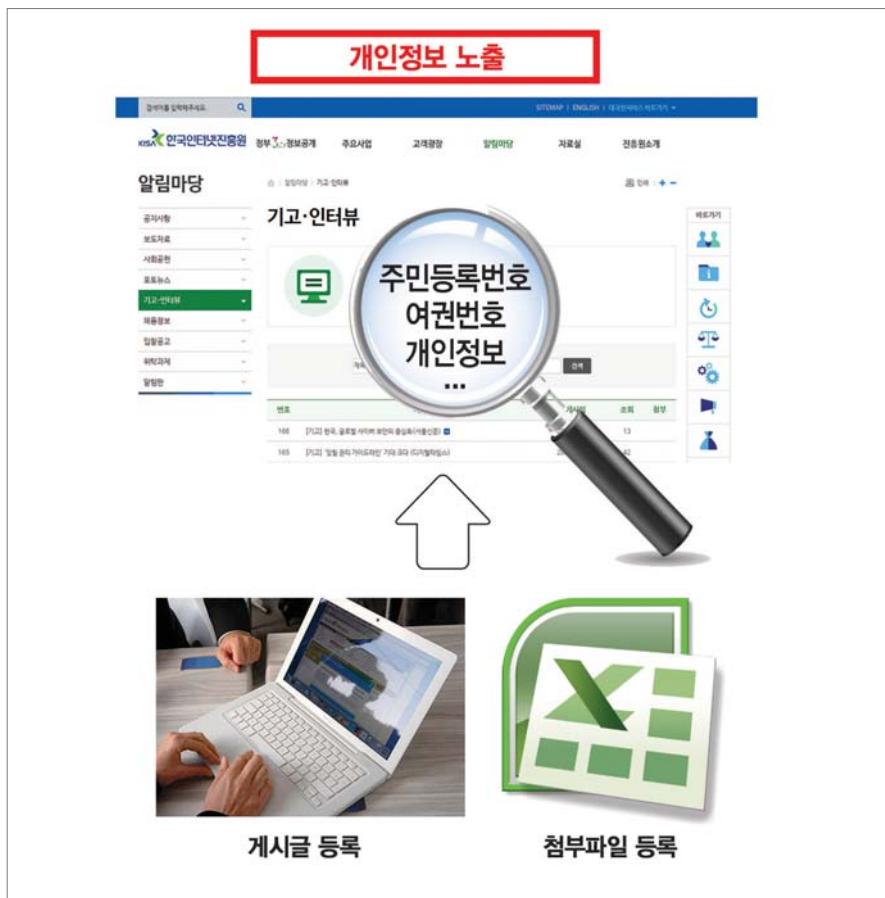
게시글에 의한 노출은 개인정보 취급자가 공지사항 작성이나 민원 처리 시 부주의하여 개인정보가 노출되거나, 또는 홈페이지 이용자가 민원을 작성하거나 예약확인 요청 등을 위해 자신의 개인정보를 공개하여 개인정보가 노출되는 경우에 발생할 수 있습니다.

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

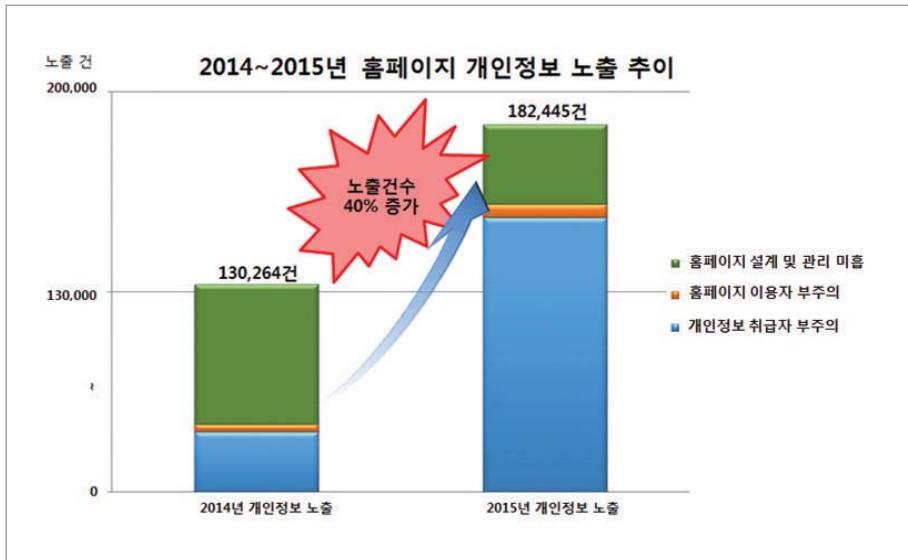
노출 원인	내 용
홈페이지 설계 및 관리 미흡	소스코드, URL, 홈페이지 취약점 등에 의해 개인정보가 노출되는 경우
첨부파일 노출	홈페이지에 개인정보가 포함된 첨부파일을 업로드 하는 경우
게시글 노출	홈페이지에 작성한 공지사항 및 댓글 등에 개인정보가 포함되어 있는 경우



[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.

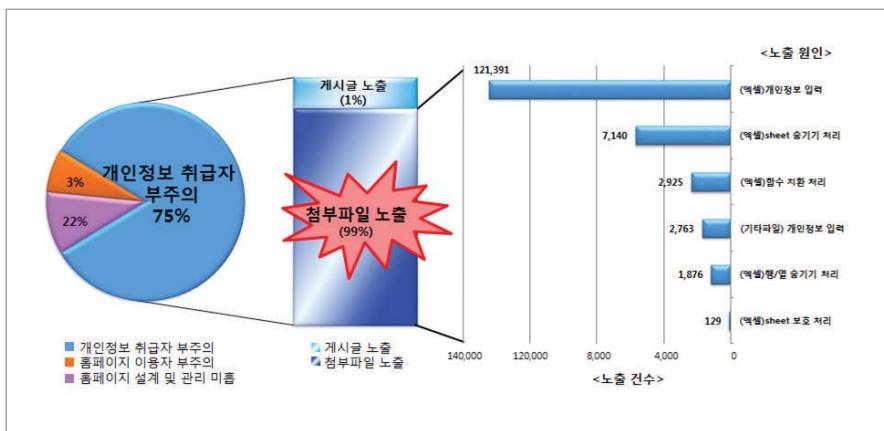


[그림 3] 2014년~2015년 홈페이지 개인정보 노출추이



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
공공 기관	중앙행정기관	<ul style="list-style-type: none"> 참여마당 '자유게시판' 글에서 주민등록번호 노출 정보조회의 '일반정보' 글에서 운전면허번호 노출 	게시글 노출
		<ul style="list-style-type: none"> 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
		<ul style="list-style-type: none"> '개별공시지가 이의신청' 첨부파일에서 주민등록번호 노출 과제검색 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출 	첨부파일 노출
	지방자치단체	<ul style="list-style-type: none"> 정보공개창 게시판의 '배출업소현황' 첨부파일에서 주민등록번호 노출 우리동소식 게시판의 '일산대상자 명단' 첨부파일에서 주민등록번호 노출 'OO시 선수명단' 파일에서 주민등록번호 노출 행정처분 명령서 파일에서 주민등록번호 노출 	첨부파일 노출
		<ul style="list-style-type: none"> '급식행정공개', '가정통신문'에서 주민등록번호 노출 행정실 게시판의 '운영위원회' 파일에서 주민등록번호 노출 부별업무자료의 '스카우트' 알집파일 내에 존재하는 첨부파일에서 주민등록번호 노출 	첨부파일 노출
		<ul style="list-style-type: none"> 민원센터의 '학사/학적변동' 글에서 주민등록번호 노출 사이버강좌의 '개설강좌' 글에서 주민등록번호 노출 	게시글 노출
	대학교	<ul style="list-style-type: none"> '여학원 수강신청' 파일에서 외국인등록번호 노출 행정실 공지사항 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출 	첨부파일 노출
		'OO대학교 관리자페이지에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
		<ul style="list-style-type: none"> '여행예약확인 요청' 글에서 주민등록번호, 여권번호 노출 '현금 영수증 요청' 글에서 주민등록번호 노출 	게시글 노출
민간 기관	여행업	<ul style="list-style-type: none"> 고객센터의 '질문과 답변' 글에서 주민등록번호 노출 이용안내의 '자주 묻는 질문 FAQ' 글에서 주민등록번호 노출 	게시글 노출
		<ul style="list-style-type: none"> 건강상담의 '복약상담' 글에서 주민등록번호 노출 	게시글 노출
		<ul style="list-style-type: none"> 정보광장의 '채용공고' 파일에서 주민등록번호 노출 요양급여비용 청구서 파일에서 주민등록번호 노출 	첨부파일 노출
	의료업	건강진단 결과표에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
		<ul style="list-style-type: none"> '개인성적기록' 조회 게시판에서 주민등록번호 노출 '참가팀 소개' 게시판에서 주민등록번호 노출 	홈페이지 설계 및 관리 미흡
		<ul style="list-style-type: none"> '자원봉사신청서' 첨부파일에서 주민등록번호 노출 내용 증명서 파일에서 주민등록번호 노출 	첨부파일 노출
	단체	'본회소개의 '회원명단' 글에서 주민등록번호 노출	게시글 노출
		<ul style="list-style-type: none"> 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 리스트팅의 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.

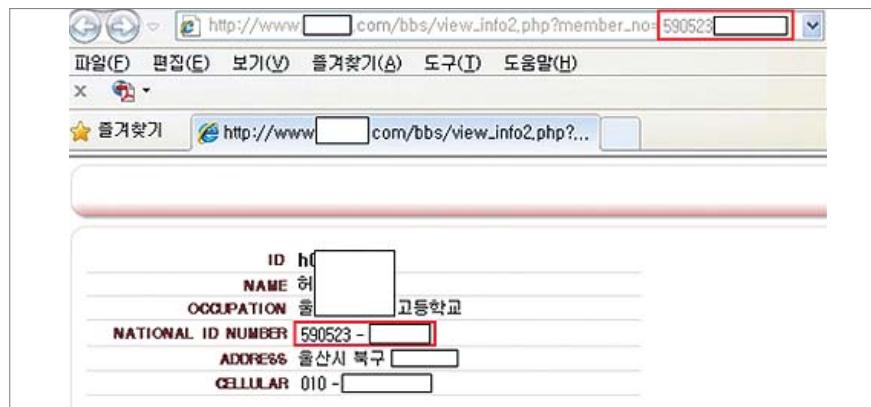
[표 4] 홈페이지 설계 및 관리 미흡으로 인한 노출 유형

노출 유형	내 용
설계 미흡	URL에 개인정보가 노출
	이용자 화면 소스코드에 개인정보가 노출
	게시글 작성 중 임시 저장 페이지에 개인정보가 노출
	디렉터리 리스트의 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.



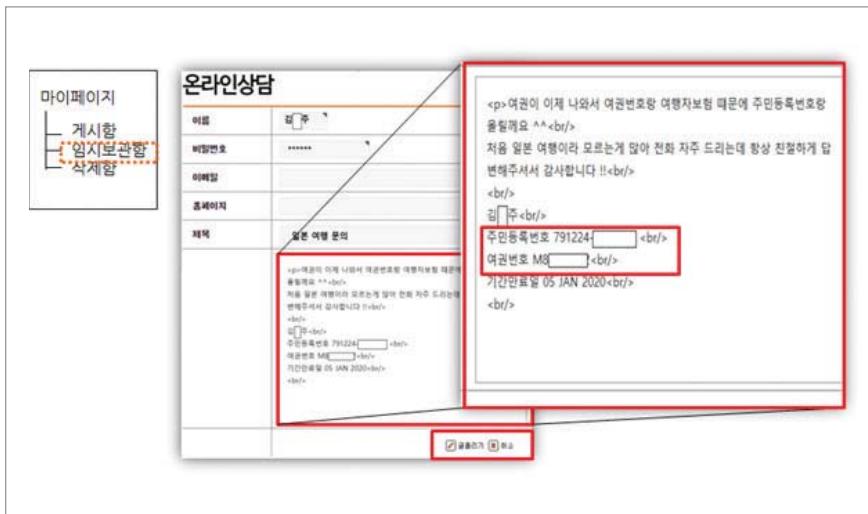
[그림 6] 소스보기에서 개인정보가 노출된 사례

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.

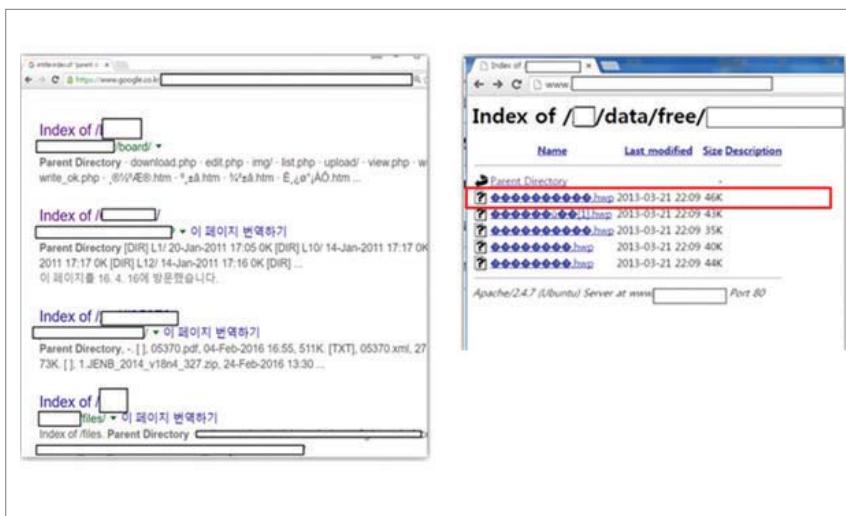


[그림 7] 임시보관함에 저장된 게시글 노출 사례



라. 디렉터리 리스트ng의 잘못된 설정으로 인해 개인정보가 노출된 사례

디렉터리 리스트ng 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 리스트ng 취약점으로 개인정보가 노출된 사례

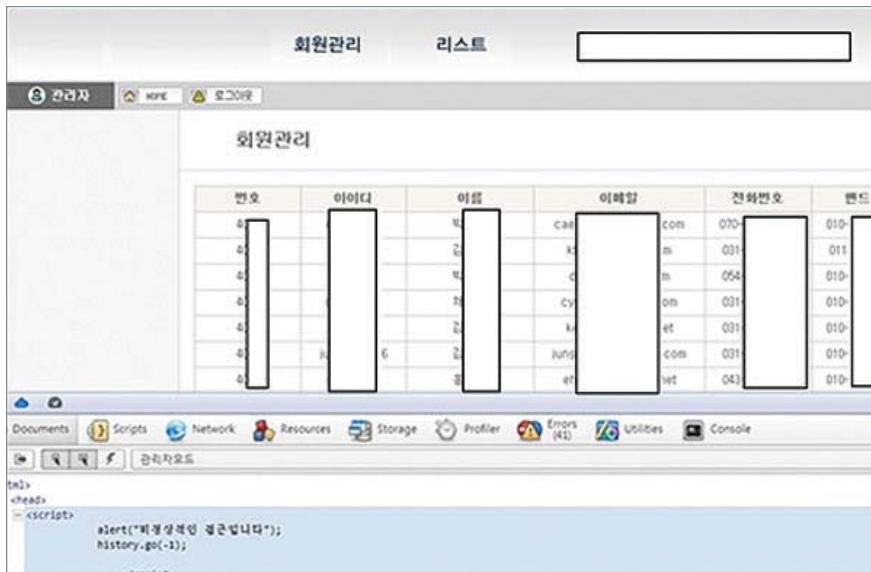
홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치방법 (예시)

- 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 네트워크에서만 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

제시판에 첨부되는 엑셀, 한글문서, PDF, 텍스트파일 등 다양한 유형의 첨부파일에 개인정보가 노출되는 경우를 말합니다. 개인정보 취급자가 공지사항 등 제시판에 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

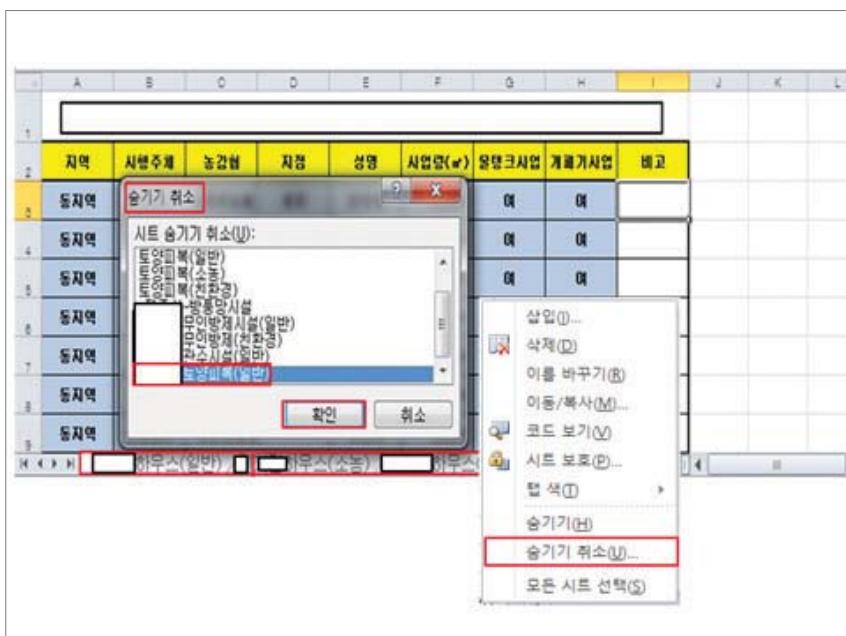
노출 유형	내 용
엑셀파일에 의한 노출	[숨기기] 기능에 의한 개인정보 노출
	시트보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보 노출
	함수 치환 후 원본 내용 미삭제로 인한 개인정보 노출
	[메모]기능으로 인한 개인정보 노출
	배경색과 같은 글자색으로 작성하여 개인정보 노출
	OLE 객체로 인한 개인정보 노출
이미지파일에 의한 노출	개인정보가 담긴 이미지형 PDF 파일에 의한 노출
	개인정보가 담긴 이미지 파일(JPG, GIF, BMP, PNG 등)에 의한 노출

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 설정 하더라도 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.

The screenshot illustrates two scenarios where personal information is not protected:

- 1. Sheet Protection (Top Left):** A red circle labeled '1' highlights the 'Protect Sheet' button in the ribbon. A red arrow points from this button to the 'Sheet Protection' dialog box, which is also highlighted with a red circle labeled '2'. The dialog box shows that protection is applied to the sheet, but it does not mention protecting specific cells.
- 2. File Search (Bottom Left):** A red circle labeled '3' highlights the 'Find & Select' dropdown menu. A red arrow points from this menu to the 'Find & Replace' dialog box, which is highlighted with a red circle labeled '4'. The dialog box shows search results for '6월 인건비' (June Salary) across multiple files, indicating that the search term is present in unprotected files.

1. 시트보호된 파일

2. 파일 검색 프로그램을 이용해서 시트보호된 파일의 개인정보 확인 가능

Name	Modified
6월 인건비 수정.xlsx	After: Today
256 510725	
259 740119	
260 580309	
261 571001	
263 520219	
265 570106	

[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.

공시송달						
연번	성명	주민등록번호	주민등록번호	체납건수	체납액	등기소
1	조	740912-	740912-*****	10	000	등기소
2	신	661002-	661002-*****	13	000	등기소
3	남	500609-	500609-*****	39	2570	등기소
4	이	730730-	730730-*****	14	000	등기소
5	영	401231-	401231-*****	14	000	등기소
6	김	760305-	760305-*****	18	000	등기소
7	손	500506-	500506-*****	22	000	등기소
8	최	480607-	480607-*****	11	000	등기소

[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 주민등록 번호를 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.

품목	업체명	대표자	전화번호	계약기간	비고
농산품	유통	이	031-XXXXXX 031-XXXXXX 031-XXXXXX 070-XXXXXX 031-XXXXXX 031-XXXXXX	2013.5.1~2014.02.28	
A	갈라내기				
B	복사				
C	붙여넣기 품선:				
D	선택하여 풀어보기				
E	선택				
F	내용 지우기				
G	필터				
H	검정				
I	이모티콘				

[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 찾았을 수 있었던 사례입니다.

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

단체탐방 조편성

조편성	성명	성별	학과(전공)	연락처
1조	손	남	영어영문	016
	양	남	정치외교	011
	김	여	사회환경시스템	011
	조	여	교육공학	010
	김	여	부동산	010
	이	남	건축공학	010
2조	이	여	행정	010
	김	여	영어영문	010
	오	여	국제무역	016
	박	여	건축	010

단체탐방 조편성

조편성	성명	성별	학과(전공)	번호	주민등록번호
1조	손	남	영어영문	016	940317-
	양	남	정치외교	011	940713-
	김	여	사회환경시스템	011	941110-
	조	여	교육공학	010	950213-
	김	여	부동산	010	950127-
	이	남	건축공학	010	940413-
2조	이	여	행정	010	940413-
	김	여	영어영문	010	941222-
	오	여	국제무역	016	941222-
	박	여	건축	010	941003-

[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)

The image shows a Microsoft Word document window. At the top, there are three circular icons: a horse, a person at a computer, and an envelope. The main content area displays a table with yellow headers and red borders around specific columns. A red circle labeled '참조 파일' (Referenced File) points to the table. A red arrow labeled 'OLE 객체삽입' (OLE Object Insertion) points from the bottom of the table to a separate window below it. This separate window contains a chart titled '학자금대출 조기상환 요인' (Factors for early repayment of student loans). The chart is a horizontal bar chart with two bars. The legend indicates four categories: 부모소득 (Parental Income), 본인소득 (Personal Income), 장학금 (Scholarship), and 학부모상환변동 (Change in repayment by parents). The first bar represents the sum of parental and personal income, while the second bar represents scholarship and its change.

연도	은행	계좌번호	출생년도	주민등록번호	핸드폰번호
2005	민	94521	81	81	01 0
2005	리	12018	80	80	01 1
2005	나	93046	49	49	01 4
2005	협	00015	77	77	01 3
2005	흥	93604	85	85	01 6
2005	나	48941	67	67	01 7
2005	협	48932	55	55	01 5
2006	리	36841	79	79	01 7
2006	나	00481	77	77	01 7
2006	민	01478	85	85	01 1
2006	리	85548	67	67	01 5
2006	나	00548	55	55	01 5
2006	협	52233	79	79	01 9
2006	흥	11147	77	77	01 7
2006	나	99467	85	85	01 B
2006	협	16575	67	67	01 1

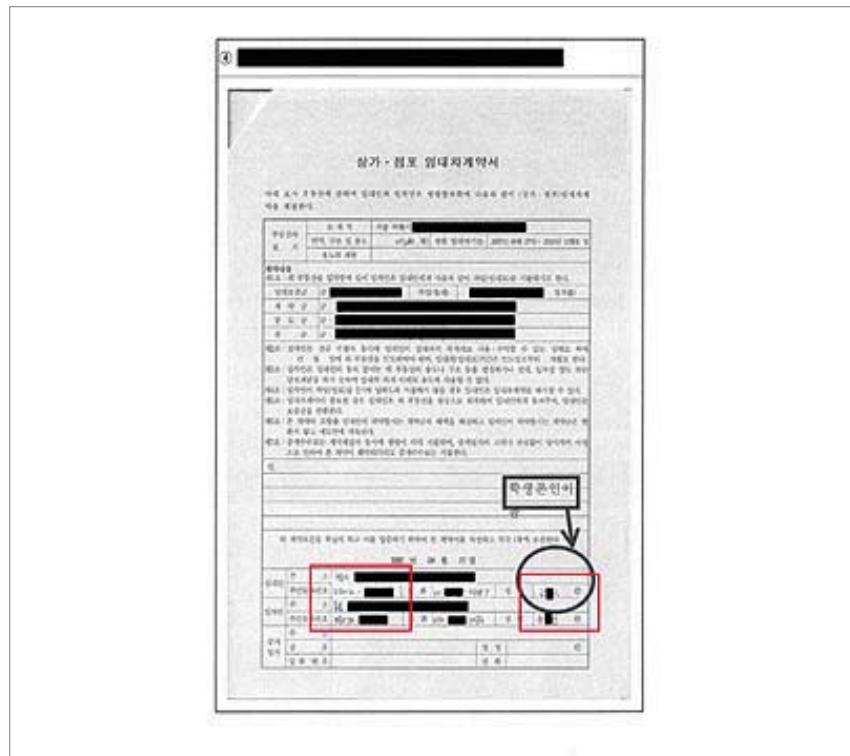
[그림 16] OLE 객체 내에 있는 개인정보 노출 사례

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 리스트링 취약점에 의해 개인정보가 노출된 사례입니다. 개인정보가 포함된 이미지 파일의 노출을 방지하려면 디렉터리 리스트링 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 가지입니다. 첫째는 게시판에 게시글(공지 사항, 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.

Q&A

제 목	<input type="text"/> 재발급 요청
작성자	이 <input type="text"/>

안녕하세요

재발급을 요청드립니다.

발급연도는 20□년 인지 20□년 물중에 한 해이고,
 □대학교 □ 대학시에 학교에서 시험보고 땄으며,
 주민등록번호는 820126-□□□이고,
 연락처는 010-9□□-7□□입니다.

[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.

선생님 궁금한 것이 있는데요.
 가 흠피에 회원가입을 하려는데
 외국인이라 주민등록번호가 외국인등록번호로 되어 있고
 입력을 하니 등록이 안 된다네요. ^^;
 어찌 등록을 해야하나요?
 정식으로 회원으로 가입하는 것도 어찌 해야하는지
 알려주세요. 히히

시간이 되시면 춘천에 꽃구경 오세요.
 제가 막국수 사드릴게요.

^^*

如心이자

메일 온 내용입니다.
 운영자와 상의해서 가입처리를 하겠습니다.

Name: Martin

ID # : 780929-5

H.P : 010-108

[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 작성률 유도하는 안내글을 삭제하고, 공개된 게시글에 등록된 개인정보는 **** 등으로 마스킹 처리하거나 삭제해야만 합니다.

또한 예약시, 영문성함, 나이, 성별, 여권번호, 전화번호, 이메일주소 등이 필요하므로 답글로 달아주시면 확인 후에 안내사항을 전달해드리도록 하겠습니다.

감사합니다.

할공□□송□□0□□421/□□428-7□□□@hanmail.net

[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)

홈페이지 개인정보 노출방지 안내서

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.

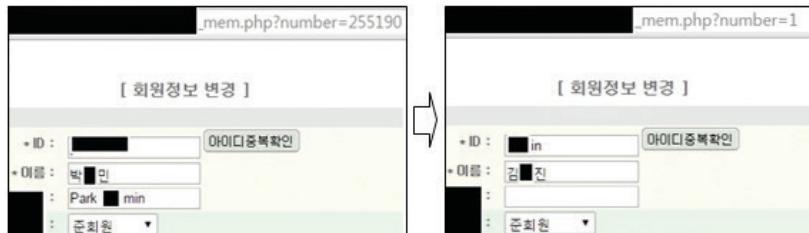
이 작업은 홈페이지의 프로그램 코드를 수정하는 것으로 개발 또는 운영 인력과 함께 처리해야 합니다.

※ 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 임의의 변경을 통해 타인의 개인정보를 열람할 수 있습니다.

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



② 전송방식 변경 및 개인 식별자 변경

```
<form action="http://www.ooo.com/bbs/view_info2.php" method="POST">
<input type="text" unique_key="A2FCDQE">
<input type="submit" value="확인">
...
</form>
```

[그림 22] URL에 개인정보가 노출된 경우 조치방법

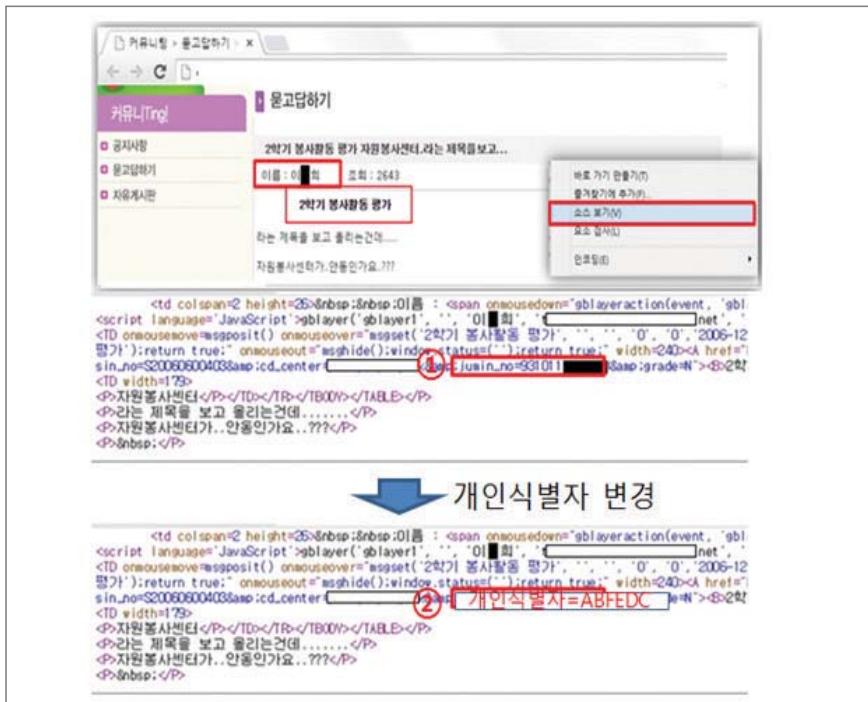
처리절차 (예시)

- 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 작성률 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	<ul style="list-style-type: none"> · 개인정보 보호조치 컨설팅 · 홈페이지 웹 취약점 점검 서비스 · 업무용PC 점검도구 제공 · 주민등록번호 미 수집, 암호화 조치 지원 	
절차/방법	<ul style="list-style-type: none"> · 우편, FAX, 이메일, 홈페이지 	
온라인신청	<ul style="list-style-type: none"> · 개인정보보호 종합포털(www.privacy.go.kr) > 사업자 > 개인정보보호 기술지원 	
문의처	<ul style="list-style-type: none"> · 한국인터넷진흥원 개인정보보호 기술지원센터 (☎ 118) 	

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

라. 디렉터리 리스트팅의 올바른 설정 방법

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

디렉터리 리스트팅

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 리스트팅 검색방법



[그림 24] 디렉터리 리스트팅 취약점이 있는 홈페이지의 검색 예시

intitle:index.of "parent directory" site:kisa.or.kr와(과) 일치하는 검색 결과가 없습니다.

제안:

- 모든 단어의 철자가 정확한지 확인하세요.
- 다른 검색어를 사용해 보세요.
- 더 일반적인 검색어를 사용해 보세요.
- 키워드 수를 줄여보세요.

[그림 25] 디렉터리 리스트팅 취약점이 없는 홈페이지의 검색 예시



UNIX 또는 LINUX 환경

- ☑ Apache : httpd.conf 파일에서 indexes 문자열 제거

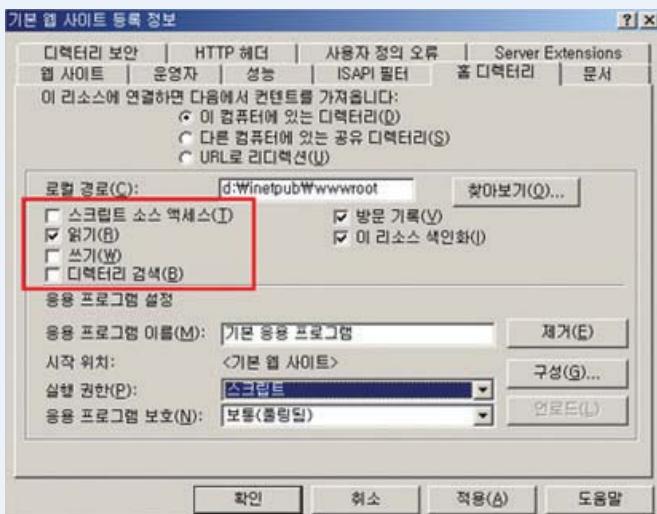
```
<Directory "/user/local/server/apache/htdocs">
    Options Indexes
</Directory>
```

- ☑ Tomcat : web.xml 파일에서 param-value false로 설정변경

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

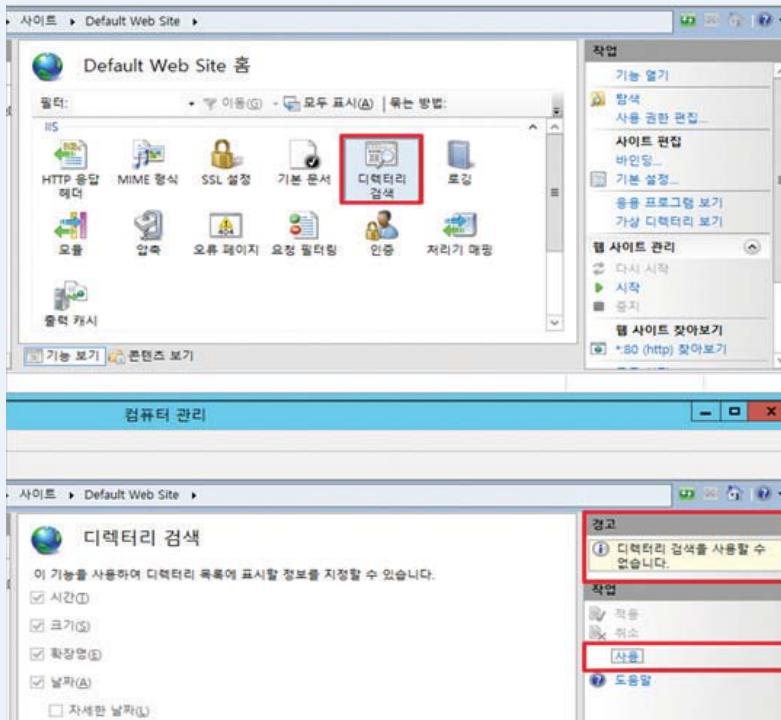
윈도우 IIS(Internet Information Service) 환경

- ☑ IIS 6.x 이하 : 제어판 → 관리도구 → 인터넷 서비스 관리자
→ 기본 홈페이지의 속성에서 디렉터리 검색 부분을 비활성화



[그림 26] IIS 6.x 이하에서 디렉터리 리스트 방지 설정

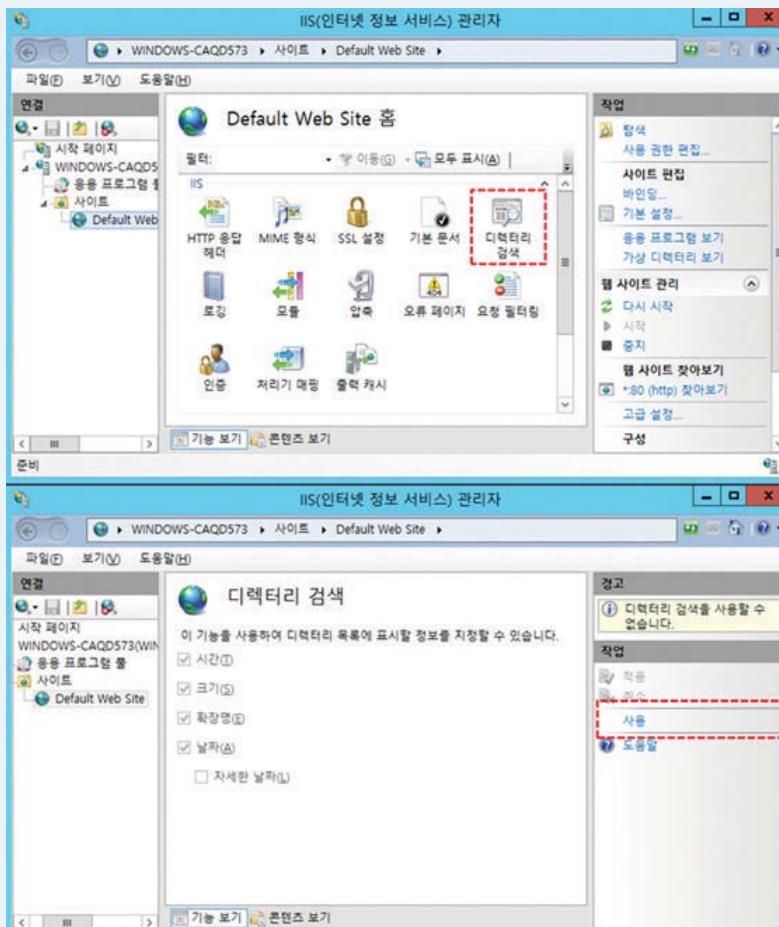
- ▣ IIS 7.x : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 홈페이지 홈 → 디렉터리 검색을 더블클릭 후 속성에서 우측 작업창에서 사용 해제



[그림 27] IIS 7.x 에서 디렉터리 리스트ng 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



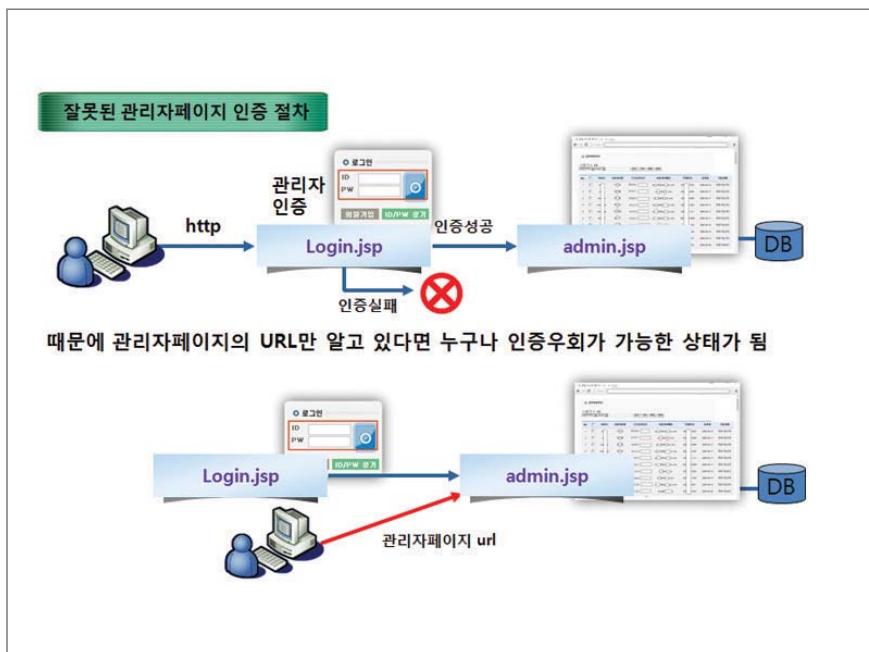
[그림 28] IIS 8.x에서 디렉터리 리스트 방지 설정

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 디렉토리(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.

No.	행정처분번호	제목	부서	작성자	상태
1	A1111111	길** 님 행정처분 결과	행정과	길보안①	비공개
2	A1111112	박** 님 행정처분 결과	정책과	길보안	공개
3	A1111113	최** 님 행정처분 결과	민원과	길보안	공개

▼

행정처분 공개

행정처분번호	20_____	인허가번호	201_____
업종명	_____	대표자명	_____
업소명	_____		
소재지	* 도로명 : * 지번명 : 서울특별시 _____ * 저본사장 : 은수호 * 저본화정일자 : 20_____ * 저본기간 : ~ * 안내사항 :		
행정처분	* 위반일자 : 20_____ * 위반사유 : ②_____ (330505-1_____) * 위반장소 :		
위반내용(1)차			
차관부서	_____과	담당자	비_____
전화번호	_____	이메일	_____

[다음]

[그림 33] 게시글/댓글 내 개인정보 노출 시 조치 절차

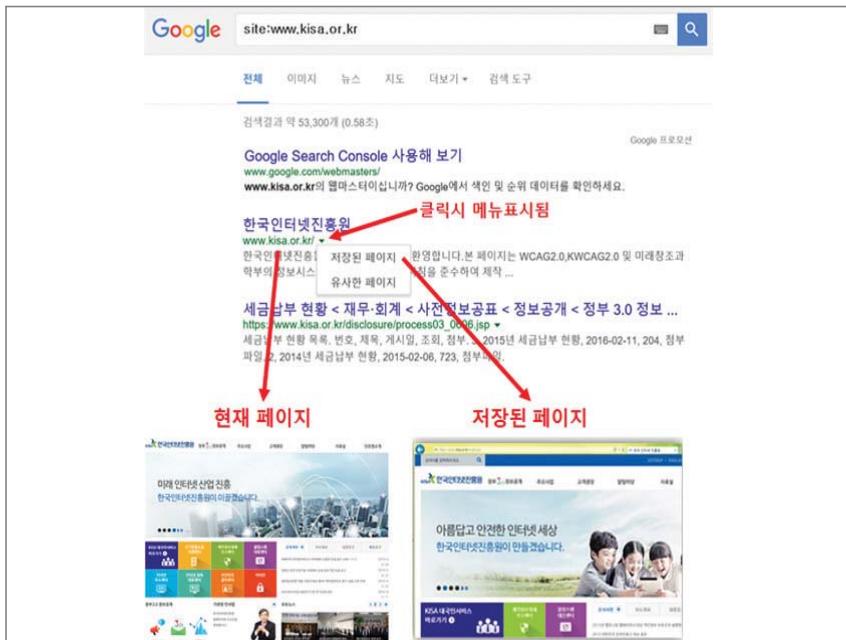
마지막으로, 노출된 페이지의 처리가 끝난 후에는 항상 검색엔진에서 해당 페이지가 수집되었는지 확인하고, 수집된 페이지가 있을 시 삭제요청을 하여야 합니다.

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.

Google에 있는 http://[REDACTED].com에 저장된 페이지입니다.
2013년 5월 13일 15:53:56 GMT에 표시된 페이지의 소樣입니다. 그동안 [REDACTED]가 변경되었을 수 있습니다. [자세히 보기]

다음 검색어가 강조표시되어 있습니다: 750020
텍스트버전

[REDACTED]입니다
구연금의 약속
알고싶어요

● 알고싶어요

공개	검색시간대 주정차 위반 아의체기
답변	답변 2013-03-22 15:05:02
아의신설서 인천사장 이름: [REDACTED] 주민등록번호: 750020-[REDACTED] 차량번호: 130-[REDACTED] 단속시간: 2013-03-22, 13:32 위반장소: [REDACTED] 단속공무원: 2-[REDACTED]-(02-[REDACTED]) 위반사항: 우측 1개창문이상 아의신설 사유: 현재 출네 주민으로써 누구보다 주위 교통장을 잘 알고 있으며 단지 내 살가식당 주차가 교통의흐름이 원활하지않아 [REDACTED] 부내피개 [REDACTED]-[REDACTED] 식당 또한 교통장의 흐름에 방해가 되지 않기에 13시를 주차 하였으나, 13:32분에 주정차 위반으로 과태료 부과를 받게 되었습니다. 그러나 [REDACTED]에서 [REDACTED] 전역 11시~14시까지 교통장의 흐름에 방해가 되지 않는 청 단속 대상에서 제외한다고 발표한 바 이의를 제기합니다. 당시 교통장 확인을 하여 살피해 주시길 바랍니다.	

[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 URL은 아래 표와 같습니다.

[표 7] 검색엔진별 캐시페이지 삭제요청 주소

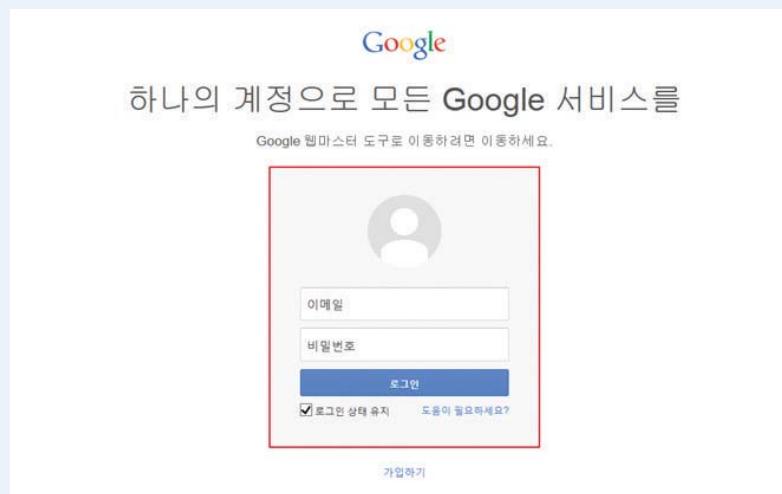
검색엔진	명칭	삭제요청 주소
구글(Google)	오래된 컨텐츠 삭제	https://www.google.com/webmasters/tools/removals
네이버(Naver)	삭제 문의 고객센터	https://help.naver.com/support/home.nhn
다음(Daum)	권리침해 신고센터	https://cs.daum.net/redbell/top.html

그리면 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)

Google

Search Console

오래된 콘텐츠 삭제

검색결과에서 삭제하려는 URL을 정확히 입력하세요. 올바른 URL 찾는 방법
일부 요청은 승인되지 않을 수도 있습니다. 이유는 다음과 같습니다.
개인정보나 법적인 문제가 있는 콘텐츠를 삭제하려면 다른 요청을 제출해야 합니다.

오래된 콘텐츠의 URL을 입력하세요. 삭제 요청

삭제 요청
전체 보기

[그림 37] 삭제 요청하기 클릭

☑ 3단계 (URL 분석 결과, 홈페이지가 삭제된 경우)

URL 분석 중

[https://\[REDACTED\]/processa03_0607.jsp](https://[REDACTED]/processa03_0607.jsp)

콘텐츠가 없습니다.

콘텐츠가 더 이상 존재하지 않거나 Google에서 차단된 것을 확인했습니다.
이제 임시 삭제 요청을 제출할 수 있습니다. 사이트 웹마스터는 Google로부터 이 URL
에 대해 오래된 페이지 삭제가 요청되었다는 알림을 받을 수 있습니다.

삭제 요청 닫기

[그림 38] 삭제 요청 클릭

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

삭제하려는 URL:
http://[REDACTED] ?document_srl=136 [?]

삭제하려는 이미지 또는 웹페이지를 사이트 소유자가 아직 삭제하지 않은 것으로 보입니다.
Google이 검색결과에서 콘텐츠를 삭제하려면 사이트 소유자가 먼저 해당 콘텐츠를 삭제하거나 업데이트해야 합니다.

이미지 또는 웹페이지가 업데이트되거나 삭제되었나요?

예 아니요

다음 **닫기**

[그림 39] '다음'으로 진행하기 클릭

5단계 (스니펫 및 캐시 삭제)

URL 분석 중

http://[REDACTED] ?document_srl=136 [?]

콘텐츠가 아직 웹에 있습니다.
Google이 검색결과에서 삭제하려면 먼저 사이트 소유자가 해당 콘텐츠를 게시 중단하거나 업데이트해야 합니다.

● 스니펫과 캐시가 오래되었습니다. Google은 페이지 사본이 오래된 경우 스니펫과 캐시를 삭제할 수 있으며, 이는 웹페이지에만 적용됩니다. 사이트 월마스터는 Google로부터 이 URL에 대해 변경된 콘텐츠 삭제가 요청되었다는 알림을 받을 수 있습니다. [자세히 알아보기](#)

전체 페이지 또는 이미지가 삭제되었습니다. [자세히 알아보기](#)

다음 **닫기**

[그림 40] '다음'으로 진행하기 클릭



▣ 6단계 (삭제하고자 하는 텍스트 입력)

URL 분석 중

http://[REDACTED]document_srl=136 ↗

콘텐츠가 아직 웹에 있습니다.
Google이 검색결과에서 삭제하려면 먼저 사이트 소유자가 해당 콘텐츠를 게시 중단하거나 업데이트해야 합니다.

콘텐츠가 어떻게 변경되었는지 알려주세요.
웹 페이지에 더 이상 표시되지 않지만 **캐시된 버전**에 표시되는 단어를 입력하세요.

삭제 요청
닫기

[그림 41] 삭제 요청 클릭

▣ 7단계 (삭제 요청 완료, 반영까지 일주일 정도 소요)

Google
Search Console

오래된 콘텐츠 삭제

검색결과에서 삭제하기 원하는 URL을 정확히 입력하세요. 좋아온 드디어 찾았습니다.
 일부 포함은 승인하지 않을 수도 있습니다. 이유는 다음과 같습니다.
개인정보나 법적인 문제가 있는 콘텐츠를 삭제하려면 다른 요청을 사용해야 합니다.

삭제된 콘텐츠의 내용을 입력하세요 ↗

삭제 요청
전체 보기 ↗

URL	상태	제거 일정	요청일
http://recon.tohome.co.kr/index.php?document_srl=136 ↗	삭제됨	연장된 콘텐츠	2016. 5. 29. 요청 외소...

[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)

웹문서

[KISA 아카데미 | 주요사업 | 한국인터넷진흥원](#)

주요사업 > KISA 아카데미사업목적 최고의 정보보호 교육 서비스 제공을 목표로, 일반인의 정보보호 인식제고 및 제작자, 대학생, 공무원 등 분야/수준별 다양한 교육 프로그램을 제공합니다....

www.kisa.or.kr/business/promotion/promotion_sub1.jsp 사이트 내 검색 | 저장된 페이지

[그림 43] 네이버(Naver) 저장된 페이지 클릭

▣ 2단계 (웹문서 삭제 요청 방법 선택)

NAVER 저정시간: 2013년 11월 20일 18:52:41 KST

아래 페이지는 네이버 웹로봇에 의하여 수집 시 저정된 페이지입니다.
페이지에 포함되어 있는 텍스트, 이미지, 동영상 등의 컨텐츠는 현재 페이지와 다를 수 있습니다.
네이버는 페이지의 작성자와 관련이 없으며 내용에 대한 책임을 지지 않습니다.

현재페이지로 이동하기 : http://www.kisa.or.kr/business/promotion/promotion_sub1.jsp
도움말 : 웹문서 수집 및 삭제 정책 | 웹문서 삭제 요청 방법

[그림 44] 네이버(Naver) 웹 문서 삭제 요청 방법 클릭

3단계 (삭제 요청)

노출 되어야 하는 내용에 대해서는 <http://WWW.NAVER.COM/NAVER/NAVER.HTML>을 확인해 주시거나,
robots.txt를 서버에 저장하고 로봇이 직접 방문하지 않는 경우라도 본인의 홈페이지 중 일부 내용 혹은 링크 같이 NAVER 접두어로 접속 결과에 나타나는 경우가
있을 수 있습니다. 이는 다른 접두어들이나 사이트들이 해당 접두어를 링크한 경우, 그 링크에 제시된 설명에 외면에서 자동적으로 생성되는 것으로, 해당 접두어의
robots.txt의 존재유무나 흐름의 동향에는 무관할 수 있습니다.

만일 이 경우에도 노출을 원하지 않는 경우에도 역시 아래의 [삭제 요청 및 문의](#)를 연락주시기 바랍니다.

3. 삭제 요청을 보내주세요.

NAVER 접두어로 접속된 내용이나 NAVER 로봇의 작동으로 인해 불편을 느끼시거나 운영에 의견이 있으신 경우, 아래의 [삭제 요청 및 문의](#)를 이용해
주시기 바랍니다. 풍상적인 경우 접수 및 확인 후 빠르면 1~2 영업일 내내 처리가 가능합니다.

여전 접두에 삭제 요청을 할 수 있으신 경우

1. 본인이 직접 홈페이지 게시물을 검색해서 제외하고 싶으신 경우
 - robots.txt를 설치하셨다면 본인뿐만 아니라 혹은 다른 라이트 같이 공유로 접두에서 게시물을 빼드릴 수 있습니다. (삭제 요청 시 robots.txt의 설치여부를 알려주세요.)
 그러나 로봇ックス를 설치할 수 없는 상황일 경우, 예를 들어 게시판 등 타 접두이지에 본인이 출판한 게시글이 걸려있는 것을 원치 않으실 경우 가장 확실한 방법은
 해당 게시글을 출판했을 때 접속하는 경로 (FTP 혹은 게시판 포트번호)로 재접속하거나 해당 게시글을 삭제하신 후, 삭제하신 본인의 URL을 (삭제 대상 URL) 네이버 고
 션터 접두에 하시는 경우입니다. [삭제 요청 및 문의](#)를 통해서 URL 접수를 하주시면 빠른 처리를 도와드립니다.

- 본인이 풀어 게시글을 비밀번호가 생각나지 않는 등의 기타 이유로 직접 삭제 할 수 없을 때 시, 먼저 사이트 운영자에게 게시글 삭제를 요청하는 것이 좋습니다.
 게시글이 삭제된 후, [삭제 요청 및 문의](#)를 통해서 URL 접수를 하시면 해당 게시글이 제외처리 할 수 있도록 배려해 드리겠습니다.

- 주민등록번호, 계좌번호, 운전면허증번호 등 치명적인 개인정보가 노출되는 페이지는 개인정보 노출에 대한 피해, 혹은 심각한 면책됨순이 우려되는 경우 원본 삭제
 과정 없이 접두에서 제외처리가 가능합니다. 그러나 신고 후 해당 글에 대한 권리 증빙을 추가로 요구할 수 있으니 이 절 알며 부탁 드립니다.

2. 운영자가 운영 중인 IP 페이지를 검색해서 제외하고 싶으신 경우
 계시만, 혹은 기관 IP 페이지를 접두에서 제외하고 싶으신 운영자의 경우 로그인, 혹은 robots.txt 설치처럼, 검색 제외 요청의사를 수집 당시에 확실히 표현하시는 것이
 가장 정확한 방법입니다. 예외적으로 이미 검색 수집을 한 후 robots.txt를 설치하신 경우에도, 요청해주시면 최대한 빠른 시간 안에 문서를 접두에서 제외시켜드립니다.
 (삭제 요청 시 robots.txt의 설치여부를 알려주세요.)
 그러나 일부 회원이 삭제를 요청하는데 운영 사정을 불가능한 경우, 일정한 권리증빙 과정을 거쳐 네이버 검색에서 제외될 수 있도록 도와드립니다.

아래의 [삭제 요청 및 문의](#)를 통해 접수해 주세요.

3. 제 3자의 게시물을 검색해서 제외하고 싶으신 경우
 본인과 관련 있는 글이라도 접두필름 하위가 접두에 되지 않는 페이지를 발견하셨거나 상인들, 약설코드 등 적합하지 않은 페이지들을 발견하면, “삭제 문의 창구”를
 이용해 신고해주세요. 여러분의 참여가 더 좋은 네이버 접두를 만들게 됩니다.

다만, 특별히 이상 있는 페이지를 신고장을 하실 경우에는, 그에 따른 합당한 근거 및 권리관계 증명이 필요하실 수 있습니다.

삭제 요청을 접수하는 데 있어 사업자를 기재해주시면 편리합니다.

- ① 본인의 이름 / 연락처 / 해당 페이지가 나오는 카페드 / 문체가 되는 게시글의 URL주소
 (여기에서 게시글의 URL은 네이버 검색결과의 URL이 아닌 각각 대상이 되는 URL로 뜻합니다)
- ② 본인과 관련된 글 혹은 운영자의 경우 문체가 또는 게시물의 권리자임을 표시하는 문서(신분증 등)의 사진 또는 그에 달라지는 자료

[삭제 요청 및 문의](#)

[그림 45] 네이버(Naver) 삭제 요청 및 문의 클릭

4단계 (삭제 사유 선택)

통합검색	
문제해결	통합검색 > 검색 결과 제외 요청하기
검색 반영 요청하기 검색 결과 제외 요청하기 원본 반영 요청하기 통합검색 정보 오류 제보 인물검색 등록 요청 인물검색 수정 요청 인물검색 삭제 요청 자동완성어, 연관검색어 등 검색어 제외 요청 네이버SEO 검색 관련 문제해결 검색 시 발생하는 강제 제보 지식N에서 문제 해결 의견 보내기	<p>제목 업데이트 조회수</p> <p>검색 결과 제외 요청하기 2014.04.17 78815</p> <p>어떤 게시물을 검색 제외하고 싶으신가요?</p> <ul style="list-style-type: none"> <input type="radio"/> 원본이 삭제된 게시물의 검색 제외를 원하는 경우 <input type="radio"/> 내가 작성한 게시물을 검색제외하고 싶은 경우 <input type="radio"/> 타인이 작성한 게시물을 검색제외하고 싶은 경우 <input type="radio"/> 채용 광고, 공모전 광고 등 정보의 시의성이 떨어져서 검색제외를 원하는 경우 <input checked="" type="radio"/> 품질성, 개인정보 노출

[그림 46] 네이버(Naver) 검색 결과 제외 요청하기 화면

5단계 (삭제요청)

아이디	로그인하기	필수입력사항
이메일	<input type="text"/>	<input type="button" value="선택"/>
작성방법안내 ①		
※ 단축URL을 기재하실 경우, 문의 접수가 어려울 수 있습니다.		
게시물 URL	게시물 URL을 정확하게 기재해 주시기 바랍니다.	
삭제 사유	검색 제외 요청 사유를 구체적으로 기재해 주세요.	
0자 입력/정답 1000자		
개인정보 수집동의	작성해주시는 이메일 정보는 문의 접수 및 고객 불만 해결을 위해 수집하여 5년간 보관합니다. <input type="checkbox"/> 동의합니다.	
<input type="button" value="작성완료"/> <input type="button" value="취소"/>		

[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.

The screenshot shows the Daum Customer Service homepage. On the left, there is a sidebar titled '권리침해 신고' (Report Abuse) with several options: '신고·진료·상황·주제' (Report, Diagnosis, Status, Topic), '복원신청' (Recovery Application), '개시자 판내' (Internal Reporter), and '명예훼손 사건 보기' (Viewing Defamation Cases). Below these are sections for '개작권 침해 신고' (Copyright Infringement Report) and '음원저작권보호요청' (Request for Protection of Soundtrack Copyright). On the right, the main content area features the Daum logo and a large graphic of a computer monitor displaying a smiley face, with three smaller smiley faces floating around it. The text on the monitor says 'Daum 권리보호 도우미' (Daum Right Protection Assistant).

[그림 48] 다음(Daum) 고객센터에서 신고하기 클릭

- ▣ 1단계 (온라인 접수 방법 선택, 오프라인 신청도 가능함)

This screenshot shows the '접수방법 선택' (Selection of Submission Method) step of the reporting process. It includes two main sections: '온라인 접수' (Online Submission) and '메일 또는 편스/우편 접수' (Email or Fax/Mail Submission). Under '온라인 접수', there is a note: '본인 명의 휴대폰이나 아이폰이 있는 경우 온라인에서 신속하게 신고할 수 있으며, 처리 진행상황을 확인할 수 있습니다.' (If you have a mobile phone or iPhone, you can quickly report online and check the processing status). Under '메일 또는 편스/우편 접수', there is a note: '서식을 다운받아 작성하신 후, 메일 또는 편스/우편으로 신고를 접수하여, 처리 진행상황 확인이 불가합니다.' (After filling out the form, send it via email or fax/postal service, and you cannot check the processing status). Both sections have a '비로가기' (View Details) button.

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

2단계 (본인 확인)

휴대폰 본인 확인	아이핀 인증 및 신규 발급
<p>회원님의 주민(외국인)번호로 가입된 휴대폰 인증을 통해 본인 확인을 진행합니다.</p> <p>갖고 계신 휴대폰은 본인 협의가 아닌 경우, 아이핀 인증을 선택해주세요.</p>	<p>회원님의 아이핀으로 본인 확인을 진행합니다.</p> <p>아이핀은 주민번호 대신 인터넷상에서 신분확인을 위해 사용할 수 있는 식별번호입니다.</p>
<p>① 휴대폰 본인 확인시 필요한 인증 비용은 모두 Daum에서 부담합니다.</p> <p>② 휴대폰 본인 확인시 입력하신 본인 확인 정보는 실명 확인 완료 후에 Daum 회원 정보에 저장됩니다.</p>	

[그림 50] 다음(Daum) 실명인증 방법 선택

3단계 (삭제 요청)

권리침해신고 > 개인정보침해 > 본인

신청인 정보 * 삭제신청인의 이름과 삭제신청 사유, 소명내용은 계시처에게 불자입니다.

✓ 이름	김□□
✓ 생년월일	1985 년 12 월 22 일
✓ 연락처	
✓ 주소	

요청내용 및 소명

✓ 게시물 주소	-문자가 된 게시물을 확인할 수 있는 정확한 URL과 글제목을 기재해주세요. -금정하신 사항과 함께 삭제조치한 글을 다룰 수 있습니다.
✓ 첨부사실 소명	-첨부내용을 구체적으로 소명해주세요. 소명내용이 없거나 부정확할 경우, 신고 내용이 반려될 수 있습니다.

첨부증거자료

파일선택 선택된 파일 없음
설명: 증거자료로 일부파일들이 있는 경우, 첨부해주세요.
설명: 일부파일이 다수인 경우, 압축하여 첨부해주세요.

0/2000KB

본인(의 대리인)은 위와 같이 첨부된 본인의 권리로 구제하기 위하여 게시물을 삭제를 신청하는 바입니다. 이후 본인의 권리가 침해되지 않은 것으로 판명될 경우에
는 게시물을 삭제 풀쳐로 만장의 주식회사 다음커뮤니케이션이 합계 되는 모든 손해를 배상할 것임을 확인합니다.
(권리침해신고의 원활한 업무처리를 위해 신고내용이 주다음 서비스에 익명처리 됩니다.)

확인

등록 취소

[그림 51] 다음(Daum) 개인정보침해 신고 삭제 요청 화면

홈페이지 개인정보 노출방지 안내서

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.

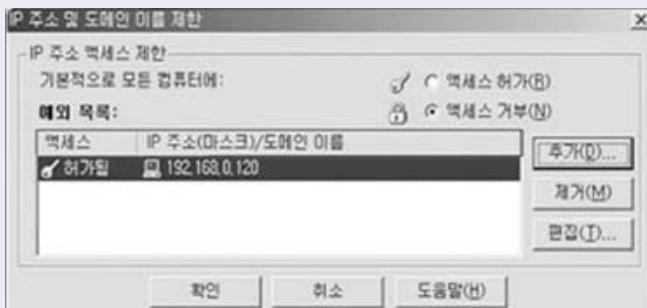
- ▣ 관리자 페이지에 외부접속이 필요할 경우, 전용선이나 가상사설망(VPN)을 이용합니다.
- ▣ 관리자 페이지는 관리자만 접속할 수 있도록 IP를 제한합니다.
- ▣ 관리자 페이지는 보안서버(SSL)를 적용하여 통신구간을 암호화합니다.
- ▣ 관리자 페이지는 인증된 관리자만 접속할 수 있도록 임의 접근을 제한합니다.
- ▣ 관리자 페이지의 주소에 추측 가능한 단어(admin, manager 등) 사용을 자제합니다.



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 이용된 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)
 - 디렉토리 리스트링 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 팁업창을 제공 합니다.

개인정보 게시에 대한 주의안내

제시된 내용 입력 및 첨부파일에 개인정보가 포함될 경우

개인정보가 유출되어 민족화 수 있으니 주의하시기 바랍니다.

FAQ

번호	제목
1120	1120개인정보보호) 스파이웨어의 설치되어 있어야 확인할 수 있는 항목이 있습니다?
1121	1121개인정보보호) “스파이웨어 설치되어 확인할 수 있는 항목이 있습니다?”
1122	1122개인정보보호) 스파이웨어 설치되어 확인할 수 있는 항목이 있습니다?
1123	1123개인정보보호) 스파이웨어 설치되어 확인할 수 있는 항목이 있습니다?
1124	1124개인정보보호) 개인정보 보호 지침을 잘 살펴보세요. 5.5. Checkin 및 확인방역관련 내용이 포함되어야 합니다!



용어 정의

이 안내서에서 사용하는 용어의 뜻은 다음과 같습니다.

용어	용어 정의
개인정보	살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영장 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 주민등록 번호, 휴대폰번호 등 개인정보가 포함되어 있는지 검사 후 차단하는 솔루션을 말합니다.
개인정보처리자	업무를 목적으로 개인정보파일을 운영하기 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.
디렉토리 (Directory)	디지털 자료 저장장치인 하드디스크에 저장된 파일들을 담고 있는 영역을 말하며, 디렉토리에는 그 속에 저장된 각각의 파일에 대한 이름과 크기, 위치 등이 기록되어 있습니다.
디렉토리 리스팅 취약점 (Directory Listing Vulnerability)	WEB이나 FTP 서비스의 취약한 설정으로 인해 서버의 디렉토리 및 파일에 열람 및 다운로드가 가능하게 되는 취약점입니다. 인터넷 이용자가 모든 디렉토리 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 향해 하기 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 시설망의 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

>>> 참고 2 OWASP에서 발표한 10대 웹 애플리케이션 보안 취약점

>>> 참고 3 구글 웹마스터 도구 사용법

>>> 참고 4 로봇배제표준

>>> 참고 5 고유식별정보 정규표현식



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)



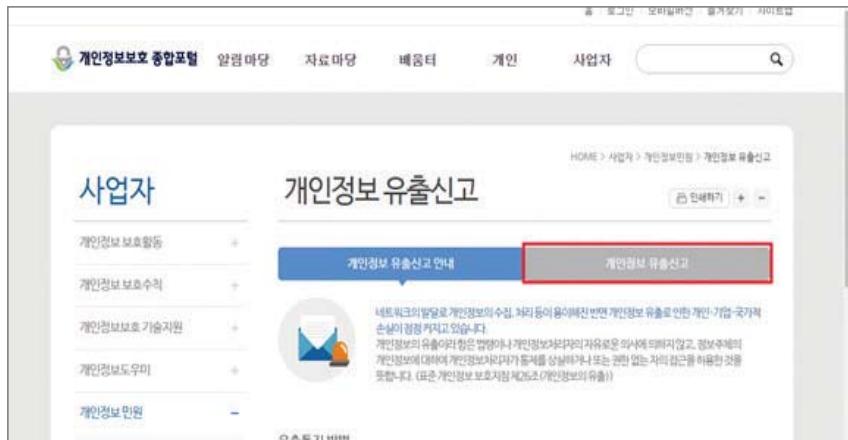
[그림 52] 개인정보보호 종합포털 화면

- ▣ 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)

HOME > 사업자 > 개인정보민원 > 개인정보 유출신고

사업자 개인정보 보호활동 개인정보 보호수칙 개인정보보호 기술지원 개인정보도우미 개인정보 민원 · 개인정보 유출신고 · 개인정보 분쟁조정 개인정보 명령령과	<h3>개인정보 유출신고</h3> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center;"> 개인정보 유출신고 안내 개인정보 유출신고 </div> <p>유출신고</p> <p>개인정보처리자는 정보주체의 개인정보가 유출된 경우(1만명 이상인 경우에는 필수이무사립~개인정보보호법 시행령 제39조 1항)에 정보주체에 대한 통지 및 조치 결과를 자체없이 신고하여야 합니다. 개인정보에 대한 침해를 신고하시려면 '개인정보 침해신고'를 이용해주시고, 개인정보 유출신고는 반드시 개인정보처리자만 신고할수록 처리됩니다.</p> <p>* 는 필수 입력항목입니다.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">신고기관 *</td> <td colspan="4"></td> </tr> <tr> <td>신고기관 유형 *</td> <td colspan="2"> <input checked="" type="radio"/> 기관 <input type="radio"/> 일반사업자 <input type="radio"/> 기자 </td> <td>통지여부 *</td> <td> <input checked="" type="radio"/> 통지 <input type="radio"/> 미통지 </td> </tr> <tr> <td>성명</td> <td colspan="4"></td> </tr> <tr> <td>연락처</td> <td colspan="4"></td> </tr> <tr> <td>이메일</td> <td colspan="4"></td> </tr> <tr> <td>유출된 개인정보의 항목 및 규모 *</td> <td colspan="4">0 / 4000 byte</td> </tr> <tr> <td>유출된 시기와 경위 *</td> <td colspan="4">0 / 4000 byte</td> </tr> <tr> <td>유출피해 최소화 대책, 조치 및 결과</td> <td colspan="4">0 / 4000 byte</td> </tr> <tr> <td>정보주체가 할 수 있는 피해 최소화 방법 및 구제절차</td> <td colspan="4">0 / 4000 byte</td> </tr> <tr> <td style="text-align: center;">성명</td> <td style="text-align: center;">부서</td> <td style="text-align: center;">직위</td> <td style="text-align: center;">연락처</td> <td style="text-align: center;">이메일</td> </tr> <tr> <td colspan="5"> 개인정보보호 책임자 * <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> </tr> </table> </td> </tr> <tr> <td colspan="5"> 개인정보취급자 * <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> </tr> </table> </td> </tr> <tr> <td colspan="5"> 유출신고접수기관은 행정자치부 및 유출신고 전문기관 담당자만 입력하시면 됩니다. 유출신고를 하시는 개인정보처리자는 입력하실 필요가 없습니다. </td> </tr> <tr> <td style="text-align: center;">기관장</td> <td style="text-align: center;">담당자명</td> <td style="text-align: center;">연락처</td> <td style="text-align: center;">이메일</td> <td></td> </tr> <tr> <td colspan="5"> 유출신고접수기관 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"><input type="text"/></td> <td style="width: 50%;"><input checked="" type="checkbox"/> 한국인터넷진흥원</td> </tr> </table> </td> </tr> <tr> <td colspan="5" style="text-align: right;"> 개인정보의 수리·이용/개인정보의 제작 </td> </tr> </table>	신고기관 *					신고기관 유형 *	<input checked="" type="radio"/> 기관 <input type="radio"/> 일반사업자 <input type="radio"/> 기자		통지여부 *	<input checked="" type="radio"/> 통지 <input type="radio"/> 미통지	성명					연락처					이메일					유출된 개인정보의 항목 및 규모 *	0 / 4000 byte				유출된 시기와 경위 *	0 / 4000 byte				유출피해 최소화 대책, 조치 및 결과	0 / 4000 byte				정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	0 / 4000 byte				성명	부서	직위	연락처	이메일	개인정보보호 책임자 * <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> </tr> </table>					<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	개인정보취급자 * <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> </tr> </table>					<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	유출신고접수기관은 행정자치부 및 유출신고 전문기관 담당자만 입력하시면 됩니다. 유출신고를 하시는 개인정보처리자는 입력하실 필요가 없습니다.					기관장	담당자명	연락처	이메일		유출신고접수기관 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"><input type="text"/></td> <td style="width: 50%;"><input checked="" type="checkbox"/> 한국인터넷진흥원</td> </tr> </table>					<input type="text"/>	<input checked="" type="checkbox"/> 한국인터넷진흥원	개인정보의 수리·이용/개인정보의 제작				
신고기관 *																																																																																											
신고기관 유형 *	<input checked="" type="radio"/> 기관 <input type="radio"/> 일반사업자 <input type="radio"/> 기자		통지여부 *	<input checked="" type="radio"/> 통지 <input type="radio"/> 미통지																																																																																							
성명																																																																																											
연락처																																																																																											
이메일																																																																																											
유출된 개인정보의 항목 및 규모 *	0 / 4000 byte																																																																																										
유출된 시기와 경위 *	0 / 4000 byte																																																																																										
유출피해 최소화 대책, 조치 및 결과	0 / 4000 byte																																																																																										
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	0 / 4000 byte																																																																																										
성명	부서	직위	연락처	이메일																																																																																							
개인정보보호 책임자 * <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> </tr> </table>					<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																																			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																																								
개인정보취급자 * <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> <td style="width: 25%;"><input type="text"/></td> </tr> </table>					<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																																			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																																								
유출신고접수기관은 행정자치부 및 유출신고 전문기관 담당자만 입력하시면 됩니다. 유출신고를 하시는 개인정보처리자는 입력하실 필요가 없습니다.																																																																																											
기관장	담당자명	연락처	이메일																																																																																								
유출신고접수기관 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"><input type="text"/></td> <td style="width: 50%;"><input checked="" type="checkbox"/> 한국인터넷진흥원</td> </tr> </table>					<input type="text"/>	<input checked="" type="checkbox"/> 한국인터넷진흥원																																																																																					
<input type="text"/>	<input checked="" type="checkbox"/> 한국인터넷진흥원																																																																																										
개인정보의 수리·이용/개인정보의 제작																																																																																											

[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 제공자들은 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 제공자들은 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 제공자들은 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)

The screenshot shows the BCC website with various service links like 'Information Disclosure', 'Complaint Reporting', and 'Information Disclosure Request'. The 'Report Center' section is highlighted, showing links for reporting telecom operators, business operators, and government bodies.

[그림 58] 사업자 개인정보 누출신고 메뉴선택

☒ 3단계 (개인정보보호 포털(www.i-privacy.kr)로 이동)

The portal's main menu includes sections for 'Business Information Disclosure', 'Information Disclosure Request', 'Information Disclosure', 'Information Disclosure', 'Information Disclosure', and 'Information Disclosure'.

[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)

· 누출신고 방법	
정보통신서비스 제공자들은 개인정보의 분실·도난·누출 사실을 안 때에는 자체 없이 방송통신위원회에 누출 관련 사항을 신고하여야 합니다.	
신고대상	건수에 관계없이 신고
신고내용	<ol style="list-style-type: none"> 1. 누출 등이 된 개인정보 항목 2. 누출 등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자등의 대응 조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
신고시기	<ol style="list-style-type: none"> 1. 정보통신서비스 제공자들이 누출 등의 사실을 인지한 시점에서 합리적인 이유 및 근거가 없는 한 즉시 신고 의무 발생 2. 추가 확인 사항은 확인되자마자 바로 신고
서면신고	<p>개인정보 누출신고서를 작성하여 전화, 팩스, 이메일, 우편으로 신고 ※ 서면신고 하신 경우 반드시 전화로 확인해 주시기 바랍니다.</p>
신고 방법	<p>개인정보 누출신고서 다운로드</p>
방송통신위원회(http://www.kcc.go.kr)	

[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 (사업지등록기준)		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 제공자들의 대응조치(필수)					
이용자가 상담 담당부서·담당자 및 연락처(필수)	성명	연락처	이메일		
	개인정보 보호책임자				
개인정보 보호담당자					
※ 하단은 접수기관에서 기재하는 부분으로 신고자는 기재하실 필요가 없습니다.					
신고 접수 기관	기관명(지역)	접수자명	연락처	이메일	접수 일자

[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)

· 누출신고 방법	
정보통신서비스 제공자들은 개인정보의 분실·도난·누출 사실을 안 때에는 자체 없이 방송통신위원회에 누출 관련 사항을 신고하여야 합니다.	
신고대상	경수에 관계없이 신고 1. 누출 등이 된 개인정보 항목 2. 누출 등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자들의 대응 조치 5. 이용자와 상담 등을 접수할 수 있는 부서 및 연락처
신고시기	1. 정보통신서비스 제공자들이 누출 등의 사실을 인지한 시점에서 합리적인 이유 및 근거가 없는 한 즉시 신고 의무 발생 2. 추가 확인 사항은 확인되자마자 바로 신고
신고 방법	서면신고 개인정보 누출신고서를 작성하여 전화, 평스, 이메일, 우편으로 신고 ※ 서면신고 하신 경우 반드시 간화로 확인해 주시기 바랍니다. 개인정보누출신고서다운로드
인터넷 신고	방송통신위원회(http://www.kcc.go.kr) 개인정보보호 포털(http://www.i-privacy.kr)의 개인정보누출신고 페이지 이용 개인정보누출신고하기

· 누출신고 기관	
기관명	방송통신위원회, 한국인터넷진흥원
홈페이지	www.kcc.go.kr , www.i-privacy.kr
이메일주소	118@kisa.or.kr
전화번호	118

[그림 63] 개인정보 누출신고하기 클릭



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

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

KISA 개인정보보호 포털

개인정보보호 소개 기술지원 개인정보 신고 개인정보보호교육 자료실 고객센터

“ 안전한 인터넷 세상을 위한 첫걸음. 개인정보보호 ”

개인정보 신고 개인정보 누출신고 개인정보 누출신고하기

개인정보신고

개인정보 누출신고

개인정보 누출신고 안내

개인정보 누출신고는 정보통신 서비스를 제공하는 사업자를 대상으로 하는 신고처로 합니다.
개인정보 누출신고는 액스플로리 80(상)의 버튼에서 사용을 권장합니다. 액스플로리 80 다운로드 바로가기

아래의 유형 중 해당되는 신고자 유형을 선택하여 신고해 주시길 바랍니다.

사업자

귀하의 회사(기관)에서
개인정보 누출이 발생하였습니까?

개인정보 누출 신고하기 바로가기

이용자

귀하의 개인정보가
도용되거나 침해 당했습니다?

개인정보 침해 신고센터 바로가기

추가신고

이미 개인정보 누출신고를 했거나 추가누출이 발생하였습니까?

개인정보 누출 추가신고 바로가기

[그림 64] 신고자 유형 선택

참고 2 OWASP¹⁾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 변조가 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 Scripting)	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, 디렉토리, 데이터베이스 기록, 키 등의 내부 구현 객체에 대한 참조 정보를 URL 또는 품 파라미터로 노출시켜서 악의적인 공격자가 이를 조작하여 인증절차 없이 다른 객체에 접속할 수 있도록 하는 취약점
A5. 보안상 잘못된 구성 (Security Misconfiguration)	애플리케이션, 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)	애플리케이션은 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.

Search Console 도움말에 오신 것을 환영합니다.

- **Search Console 시작하기**
 - Search Console이란?
 - Google을 사용하고 계신가요?
 - 웹사이트에서 Search Console 사용
 - 모바일 앱에서 Search Console 사용
 - Google 검색에 대해 자세히 알아보기
 - Google 검색에서 콘텐츠 식별
 - 업데이트 Search Console
- + 기본사항으로 시작합니다.
- + 보고서 및 기능 사용
- + 검색하기 쉬운 콘텐츠 작성하기
- + 웹마스터 아카데미

Search Console 교육 리소스

검색엔진 최적화 기본 가이드
검색엔진이 내 콘텐츠를 더 쉽게 크롤링, 색인 생성, 이해할 수 있도록 광장사항을 활용하여 더 많은 잡제고객을 유치하세요.

Google 웹마스터 포럼
Google 웹마스터 도구 포럼에서 다른 웹마스터 및 최우수 사용자와 교류.

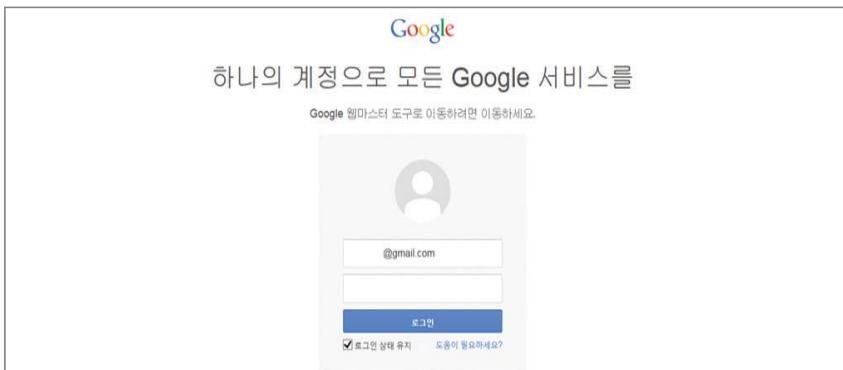
[그림 65] 구글 웹마스터 도구 도움말 접속 화면

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)

Google

Search Console

http://www.example.com/.의 소유권 확인 자세히 알아보기

권장 방법 대체 방법

권장 방법: HTML 파일 업로드

사이트에 HTML 파일 업로드

- 이 HTML 확인 파일을 다운로드합니다. [google03ebefef6b1a62eb.html]
- http://www.example.com/에 인증 파일을 업로드합니다.
- 브라우저에서 http://www.example.com/google03ebefef6b1a62eb.html 을(를) 방문하여 업로드에 성공했는지 확인합니다.
- 아래에서 '확인'을 클릭하세요.

확인된 상태를 유지하려면 확인이 완료된 후에도 HTML 파일을 삭제하지 마시기 바랍니다.

확인 나중에

[그림 69] HTML 파일 업로드

☒ 5단계 (사이트 추가 완료)

Google

Search Console

정렬 사이트 상태순 알파벳순

kisatest.bl.ee

사이트 추가

사이트 관리

전체 메시지

기타 리소스

새 메시지나 최근에 발생한 중요한 문제가 없습니다.

[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 (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	사이트소유권확인 필요
URL 삭제	긴급하게 사이트를 구글 검색결과에서 삭제하는 기능 (주의) 글 검색결과에서 일시적으로 제외하는 방법이므로 홈페이지조차 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 (예시) 홈페이지에서는 삭제되었지만, 캐시에 개인정보가 노출된 경우	사이트 소유권 확인 필요 없음

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.

The Meaning of the Talking Heads Song "This Must Be The Place ...
www.newyorker.com/.../the-talking-heads-song-that-explains-talking-he... ▾
Jun 14, 2012 - In Jonathan Lethem's new book, "Fear of Music," a study of the Talking Heads album by the same name and a riff on his emotional history with ...

줄임표가 있는 URL은 복사하여 붙여 넣지 마십시오. 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 마십시오.

▣ 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)

The screenshot shows the 'Search Console' dashboard. On the left, there's a sidebar with various metrics like '검색 노출' and 'Fetch As Google'. The main area has sections for '최신 및 중요' (Latest and Important) and '현재 상태' (Current Status). Under '현재 상태', there's a box for '크롤링 오류' (Crawling Errors) which says '최근 90일간 감지된 오류가 없습니다. 멋지군요!' (No errors detected in the last 90 days. Great!). A red box highlights the 'Fetch As Google' button at the bottom of the sidebar.

[그림 72] 'Fetch As Google' 클릭

☒ 3단계 (사이트 주소 입력)

This screenshot shows the 'Fetch As Google' interface. It has a sidebar with 'Fetch As Google' selected. The main area has a text input field containing 'http://kisatest.firebaseio.com/'. Below the input field is a note: '페이지를 가져오려면 URL을 입력합니다. 조합을 취하는 대로 한 번 정도 달라 수 있습니다.' (Enter the URL to fetch the page. The combination may change once or twice). There are two red buttons at the bottom: '제작오기' (Fetch) and '제작오기 및 맨다라' (Fetch and Mandala).

[그림 73] 사이트 주소 입력 후 '가져오기' 클릭

☒ 4단계 (사이트 재수집 요청)

This screenshot shows the results of the fetch request. It has a sidebar with 'Fetch As Google' selected. The main area displays a table with one row. The table columns are '경로' (Path), 'Googlebot 유형' (Googlebot Type), '맨다라 요청일' (Mandala Request Date), and '상태' (Status). The path is '/'. The Googlebot type is '맨다라'. The曼陀羅請求日 is '14.10.1 오전 10:22'. The status is '체크됨' (checked). A red box highlights the '체크됨' button.

[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)

URL	Googlebot 응답	가짜로기 상태
□ http://test.kisatest.bl.ee/	응답	색인에 적용되는 URL 및 참조 페이지
□ http://test.kisatest.bl.ee/	응답	색인에 적용되는 URL 및 참조 페이지

[그림 76] 삭제 신청 및 확인



라. URL 삭제 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 검색 결과에서는 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

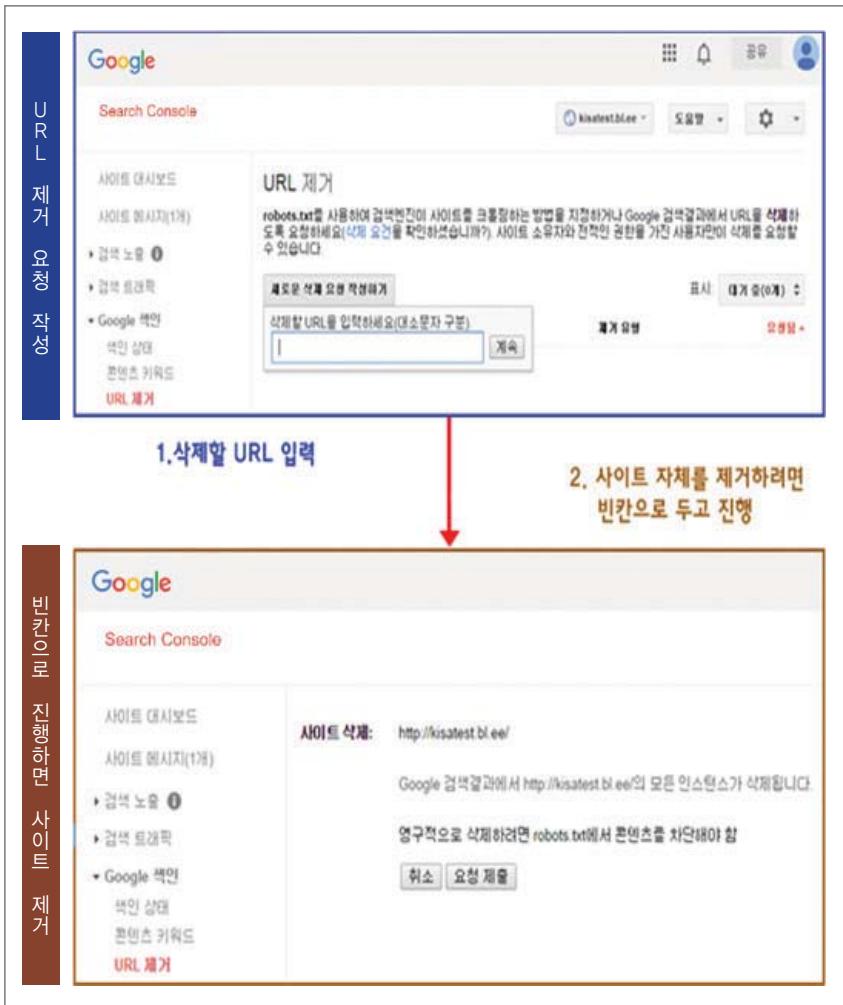
☒ 2단계 (URL 제거 도구 선택)

[그림 78] ‘URL 제거’ 선택 클릭

☒ 3단계 (삭제 요청)

[그림 79] ‘새로운 삭제 요청 작성하기’ 클릭

☒ 4단계 (삭제할 URL 입력, 사이트 자체를 제거하려면 빙Carl으로 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(디렉토리, 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. 로봇제표준 적용 시 유의점

로봇제표준은 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. 로봇제표준 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.

로봇제표준 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 파일 이름	robot.txt ※ 설정파일 이름은 “robots.txt”로 해야함	robots.txt
설정파일 적용 위치	example.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]{2}[~.[:space;]][0-9]{3}[~.[:space;]][0-9]{2}|[0-9]{2}[~.[:space;]][0-9]{2}|
[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}|[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