

홈페이지 개인정보 노출방지 안내서

2020. 12



2020. 12.

홈페이지 개인정보 노출방지 안내서



- 본 안내서는 「개인정보 보호법」 등 관계 법령의 규정을 토대로,
 - 개인정보처리자 등을 대상으로 인터넷에 노출된 개인정보의 오남용을 예방하기 위하여 개인정보 노출 원인별 구체적인 사례 및 조치방법에 대한 올바른 이해를 돕기 위한 목적으로 발간하였습니다.
- 본 안내서에서 제공하는 조치방법 및 처리절차 사례 등은 각 기관의 고유한 특성 및 실제 환경에 맞게 적용하시면 됩니다.

◆ 본 안내서의 파일은 '개인정보보호 포털' 홈페이지에 게시되어 있습니다.

홈페이지 개인정보 노출방지 안내서



제·개정 이력

본 『홈페이지 개인정보 노출방지 안내서』는 2008년 2월 제정 이후 7차 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	
6차 개정	2018.11	
7차 개정	2020.12	

CONTENTS

I 개요	1. 개인정보란?	8
	여기서, 잠깐! ▶ 일상생활에서 다양하게 활용되는 개인정보	10
	2. 개인정보 노출의 이해	11
	가. 개인정보 노출의 개념 및 위험성	11
	나. 언론보도로 보는 개인정보 유·노출	14
	다. 숫자로 보는 개인정보 노출	19
II 개인정보 노출 원인 및 조치방안	1. 홈페이지 운영·관리자 부주의에 의한 노출	25
	가. 개인정보가 포함된 게시물 및 댓글 게시	25
	나. 개인정보가 포함된 첨부파일 게시	28
	여기서, 잠깐! ▶ 개인정보 노출의 원인이 되는 엑셀 기능 알아두기	34
	2. 이용자 부주의에 의한 개인정보 노출	51
	가. 개인정보가 포함된 게시물 및 댓글 작성	51
	나. 개인정보가 포함된 첨부파일 게시	54
	3. 홈페이지 설계 및 개발 오류에 의한 노출	57
	가. 관리자페이지 접근제어 미흡	57
	여기서, 잠깐! ▶ 관리자페이지 안전하게 보호하기	59
	나. 홈페이지 접속경로(URL) 관련 오류	63
	여기서, 잠깐! ▶ GET 방식과 POST 방식 알아보기	66
	다. 홈페이지 소스코드 보안설정 미흡	68

라. 임시 저장 페이지 미삭제	70
마. 디렉터리 리스팅 보안설정 미흡	71
4. 검색엔진을 통한 개인정보 2차 노출	74
가. 검색엔진의 이해	74
나. 검색엔진을 통한 2차 노출 방지 방안	75

III
개인정보
노출
예방수칙

1. 홈페이지 운영·관리자 개인정보 노출 예방수칙	94
2. 홈페이지 개발자 개인정보 노출 예방수칙	98

FAQ

무엇이든 물어보세요	108
------------	-----

부록

[부록 1] 주요 용어 이해하기	120
[부록 2] 개인정보 노출 점검, 스스로 해보기	123
[부록 3] 개인정보 유출 시 필수 조치사항	126
[부록 4] 주요 개인정보 8종 정규표현식	134
[부록 5] 참고자료	135

**홈페이지
개인정보
노출방지
안내서**

개요

1. 개인정보란?
2. 개인정보 노출의 이해

I

개요

1. 개인정보란?

‘개인정보’란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말하며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보가 포함된다.

이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려해야 한다. 또한 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 가명처리한 정보 즉, 가명정보도 개인정보에 포함된다.

(「개인정보 보호법」 제2조제1호)

개인정보는 성명, 주민등록번호, 생년월일, 주소, 전화번호 등의 기본 인적사항에서부터 민족 또는 인종에 관한 정보와 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 생체인식정보, 의료·건강정보, 학력·성적 등 교육정보, 소득·신용등급 등 금융·신용정보, 사회·경제적 지위와 정치적 성향과 같은 내면의 비밀에 이르기까지 그 종류가 매우 다양하고 폭넓다. 또한, 기관·기업에서 운영하는 홈페이지 등에

회원으로 가입하거나 등록할 때 이용자로부터 직접 수집하는 정보 뿐만 아니라, 이용자가 홈페이지나 서비스를 이용하는 과정에서 자동 생성되는 접속기록(로그), 통화내역, 상품 구매내역, GPS 위치정보 등도 개인정보가 될 수 있다.

그림 1 개인정보 종류



여기서, 잠깐!

일상생활에서 다양하게 활용되는 개인정보

그림 2 일상생활에서 개인정보의 활용



2. 개인정보 노출의 이해

가. 개인정보 노출의 개념 및 위험성

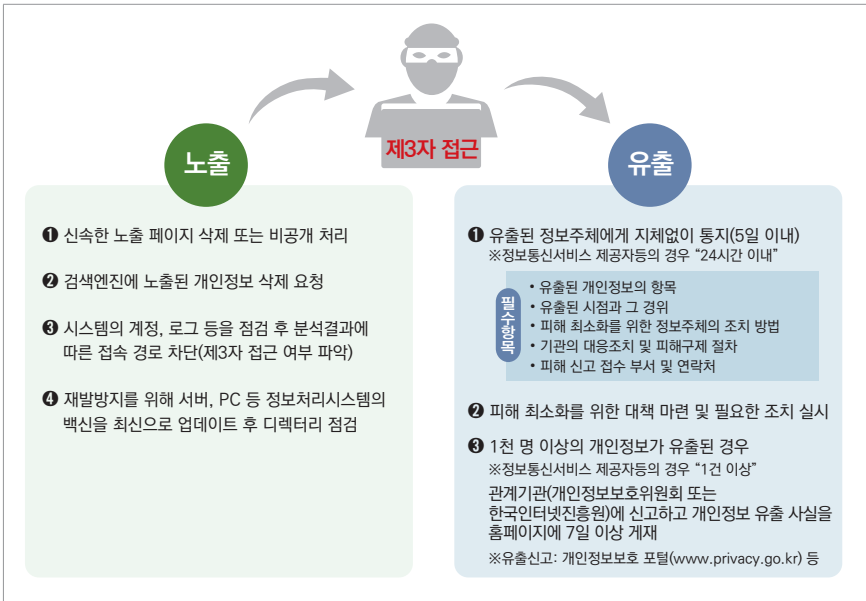
개인정보 노출이란 홈페이지 상 개인정보를 누구든지 알아볼 수 있어 언제든지 유출로 이어질 수 있는 상태를 말한다. 개인정보가 포함된 게시물이 누구든지 알아볼 수 있는 상태로 등록된 경우, 이용자 문의 댓글에 개인정보가 공개된 경우, 개인정보가 포함된 첨부파일을 홈페이지 상에 게시한 경우 등을 예로 들 수 있다.

한편, 개인정보 유출이란 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다 [표준 개인정보 보호지침 제25조(개인정보의 유출)].

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

개인정보 노출과 유출의 가장 큰 차이점은 권한 없는 자의 접근이 이루어졌는지 여부이다. 단순히 게시판에 개인정보가 게시되어 있다면 노출에 해당하지만 권한 없는 자의 접근이 이루어지거나 개인정보를 다운로드 하였다면 이는 유출에 해당한다. 개인정보가 노출되었다면 이를 신속하게 삭제하거나 비공개 처리해야 하며, 권한 없는 제3자가 개인정보에 접근하여 유출로 판단된다면 정보주체에게 유출통지하고 관계기관에 신고하는 등 개인정보 보호법 제34조(개인정보 유출 통지 등) 및 개인정보 보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)에 따른 조치를 취해야 한다.

그림 3 개인정보 유·노출 시 조치사항

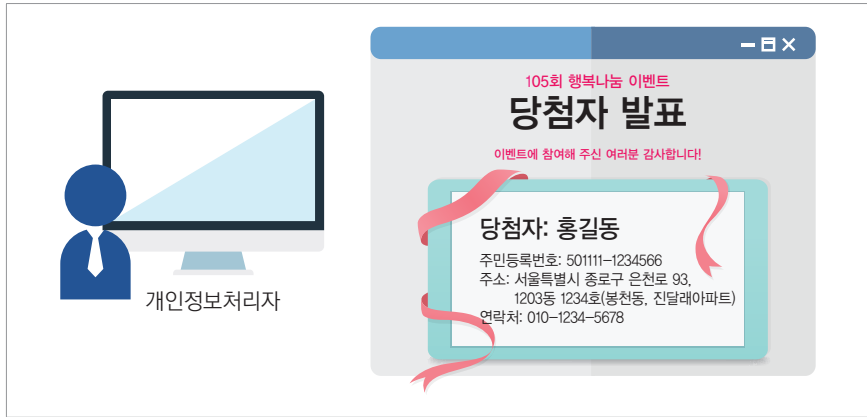


본 안내서의 조치방법은 노출 시, 유출을 예방하기 위한 최소한의 필수 조치로 시스템 로그 분석, 노출 게시물 조회 수, 노출 기간 등을 종합적으로 검토·분석하여 제3자가 개인정보를 열람·조회·다운로드 등을 하였다면 개인정보 보호법 제34조 및 제39조의4에 따른 통지·신고 등의 조치를 취하여야 한다.

인터넷 활용이 증가함에 따라 온라인 상 노출되는 개인정보는 이름, 생년월일, 주소, 전화번호, 이메일 주소 등의 기본정보 뿐만 아니라, 주민등록번호 및 여권번호, 운전면허번호, 외국인등록번호와 같은 고유식별정보, 더 나아가 통장 계좌번호, 신용카드번호, 건강보험번호 등에 이르기까지 매우 다양하게 나타나고 있다.

개인정보 노출이 발생한 후 신속히 조치하지 않아 유출사고로 이어질 시, 개인의 경우 사생활침해, 명의도용, 불법스팸, 보이스피싱 등에 의한 경제적·정신적 피해를 야기할 뿐만 아니라 유출된 개인정보가 각종 범죄에 악용될 우려가 있으며, 기관·기업의 경우에도 고객 신뢰 상실, 이미지 실추, 소비자단체 등의 불매운동, 더 나아가 소송이나 손해배상 등 유·무형의 피해를 입을 수 있다.

그림 4 개인정보 노출의 사례



개인정보처리자는 홈페이지에서 처리하는 개인정보의 처리방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험성을 고려하여 개인정보를 안전하게 관리하여야 한다. 따라서 홈페이지를 운영하는 기관·기업에서는 내부 직원 교육을 통한 인식 제고와 함께 홈페이지 상 개인정보 작성 시 주의 안내, 지속적인 노출 모니터링 실시 등 각별한 주의가 필요하다. 특히 정보통신서비스 제공자 등에 대하여는 일반 개인정보처리자와 구분하여 개인정보 보호법 제39조의10에서 노출된 개인정보의 삭제·차단 의무조치를 규정하고 있다.

참고 「개인정보 보호법」 상의 개인정보 노출 관련 조항

제3조(개인정보 보호 원칙) ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

제39조의10(노출된 개인정보의 삭제·차단) ① 정보통신서비스 제공자 등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다.

② 제1항에도 불구하고 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우 정보통신서비스 제공자 등은 삭제·차단 등 필요한 조치를 취하여야 한다.

※ 자세한 개인정보 유출 통지·신고 등의 방법은 [부록 3] 개인정보 유출 시 필수 조치사항(p.126) 참조

나. 언론보도로 보는 개인정보 유·노출

※ 언론 보도에서의 유·노출 판단은 해당 언론사의 기준으로 실제 유출 여부와 다를 수 있음

2019년 12월 27일

면접 안내 메일에 개인정보 줄줄... 관리 허술



[기자] OO기업이 채용 면접을 앞둔 사람에게 안내 메일을 보내면서, 다른 응시자들 개인정보가 담긴 파일까지 함께 보냈습니다. 잘못해놓고 바로 인정하지도 않았습니다. OO기업 계열사 공채시험에 지원한 A씨가 이메일로 받은 면접 안내 엑셀 파일입니다. 면접을 볼 90여 명의 이름과 생년월일이 적혀 있는데, 화면 상단 파일명을 다른 창에 입력한 뒤 마우스를 움직이자 지원자 전체의 학력과 주소가 뜹니다.

[A씨/공채 지원자] 민감할 수 있는 학력과 집 주소 같은 내용이 포함돼 있다는 사실을 알았을 때 좀 당황스러워서 회사에 이야기했는데, 어떤 문제가 되냐 말하면서...

[기자] 직접 드러나지 않았지만 이렇게 간단한 단계를 거치니 개인정보가 그대로 노출된 것입니다. A씨는 열흘 전 회사 측에 개인정보 유출 사실을 알렸지만 아무런 조치가 없었습니다. 회사 측은 직접 개인정보를 노출시킨 게 아닌 만큼 잘못된 게 없다고 버티고 있습니다. 하지만 간단한 조작만 하면 정보가 노출되는 이런 사고도 개인정보 유출에 해당된다고 한국인터넷진흥원이 판단했고, 그제서야 회사 측은 잘못을 인정하고 조치에 나섰습니다.

[회사 관계자] 저희가 잘못된 거고, 피해자분들한테는 무조건적인 사과를 진행하고, 이제 피해가 확산되지 않도록 조금 발 빠르게 대응을 준비하고 있습니다.

[기자] 회사가 개인정보 유출사실을 알고도 이 사실을 피해자에게 알리지 않으면 5천만 원 이하의 과태료가 부과될 수 있습니다. 지난 5월 입사지원자의 개인정보를 유출한 OO에게 법원은 정신적 피해를 배상하라고 판결했습니다. 최근엔 검찰이 성추행 피해자의 연락처를 가해자에게 유출한 해당한 일도 있었습니다.

[강유희/변호사] 개인정보가 유출됐고 이로 인해 정신적 손해가 발생하면 그 위자료를 민사 소송으로 청구할 수 있습니다. 피해 발생 이후에 어떤 조치를 했는지 등을 살펴서 위자료 액수가 최종적으로 정해지게 됩니다.

출처 : SBS뉴스 https://news.sbs.co.kr/news/endPage.do?news_id=N1005580235
전반석 기자 jbs@sbs.co.kr

2019년 06월 04일

○○소방본부, 구급차 이용 시민 5천여 명 개인정보 노출 물의

'구급활동 통계' 게시 과정에서 담당자 실수로 원본 파일 올려



○○시 소방안전본부가 119구급대를 이용한 시민 5천여 명의 개인정보 일부를 본부 홈페이지에 5개월여 동안 노출한 것으로 드러났다.

4일 ○○시 소방안전본부에 따르면 지난해 말 119구급대 이용 현황을 담은 '구급활동 통계'를 홈페이지에 게시하는 과정에서 담당자 실수로 엉뚱한 파일을 올렸다.

파일에는 119구급대를 이용한 시민 5천297명의 이름과 주소, 성별, 생년월일 등 개인정보가 들어 있었다. 환자 발생 유형, 의식상태, 동공 반응, 구급대원 평가소견, 이송병원 등 9개의 건강정보 항목도 포함됐다.

소방안전본부는 지난 5월 이 같은 사실을 제보 받은 한국인터넷진흥원이 ○○시에 통보하면서 뒤늦게 확인하고 지난달 29일에야 해당 첨부파일을 삭제했다.

소방안전본부는 1천건 이상의 개인정보가 노출되면 신고하도록 한 개인정보 보호법에 따라 곧바로 행정안전부와 한국인터넷진흥원에 이 같은 사실을 알리고 홈페이지에도 공고문을 올렸다.

노출된 사람 중 주소지가 확인된 2천973명에게 등기우편을 발송해 개인정보 일부 노출 사실을 알렸다.

소방안전본부는 이날 현재까지 개인정보 노출로 인한 피해 사례는 발생하지 않은 것으로 파악하고 있다고 설명했다.

○○시 소방안전본부 관계자는 "담당자가 구급활동 통계 파일을 올리는 과정에서 실수로 원본 파일을 게시한 것으로 파악됐다"며 "앞으로 유사한 사고가 발생하지 않도록 주의하겠다"고 말했다.

2018년 07월 16일

구청 홈페이지 신분증·통장 정보 ‘줄줄’... 암호만 걸어놓았어도!



[앵커] 공공기관이라 믿고 맡긴 내 정보, 잠금 장치 없는 금고에 담긴 것처럼 보관되고 있다면 어떻게 하시겠습니까? 관공서 홈페이지에서 개인정보가 담긴 문서들이 기본적인 암호도 걸려있지 않은 채 무방비로 노출되어 있었습니다.

[리포트] 구글에서 문서를 검색하던 신씨 OO구청의 문서 다운로드 페이지에 접속했다 깜짝 놀랐습니다. 해당 인터넷 주소에 번호 한 자리만 바꿔 넣었더니 모르는 사람의 신분증 이미지가 그대로 저장된 겁니다.

[신씨] 관공서를 믿고 맡긴 개인정보인데 그것에 대한 관리 소홀로 인해 유출이 있다면 개인으로서는 너무나 큰 실망감을 감출수가 없겠죠.

[리포트] 실제 아무 번호나 입력해도 개인정보가 담긴 서류를 내려 받을 수 있습니다. 이 안에는 주민등록번호와 사진이 담긴 장애인, 기초생활 수급자 증명서는 물론 계좌번호와 서명이 담긴 통장 사본도 포함돼 있습니다. 모두 OO구민들이 제출한 자료들로 보이스피싱이나 명의도용 같은 범죄에 악용될 수도 있는 정보들입니다. 왜 이런 일이 벌어진 걸까? OO구청 측은 신분증 복사본 같은 이미지 파일을 암호화할 수 있는 시스템을 갖추고 있지 못하다고 털어놨습니다. 전문가들은 잠금장치 없는 금고에 돈을 넣어둔 것과 마찬가지라고 지적합니다.

[사이버보안학 교수] 개인정보 파일에 대해서 또는 데이터베이스에 대해서 암호화가 의무적인 사항입니다. 보안상으로는 위급해서 항상 매년 일반 점검에서 지켜라라고 하는건데...

[리포트] 최근 6년 동안 공공기관 홈페이지에서 유출된 개인정보는 모두 79만여 건. 국민들이 믿고 맡긴 개인정보가 방치되고 있는 것 아니냐는 비판이 나오는 이유입니다.

2018년 07월 02일

A여행사, 여권번호, 신용카드 등 개인정보 줄줄이 노출

특정 여행사 사이트 여권번호,카드번호,연락처,이름 등 개인정보 무방비 노출



국내 여행사 사이트에서 여권번호·카드번호·연락처 등 중요한 개인정보가 노출되는 사건이 발생했다. 특히, 개인정보는 암호화되지 않고 여행사 홈페이지를 비롯해 구글 검색 등을 통해 그대로 노출된 것으로 드러났다. 더욱이 해당 여행사의 웹사이트에 지난 2015년부터 저장돼 있었다는 의혹까지 제기되면서 개인정보 관리 부실이 또 다시 도마 위에 올랐다.

(생략)

문제가 된 해당 여행사의 예약확인 화면을 본지가 확인한 결과, 카드 결제금액, 승인번호 8자리, 카드번호, 카드 유효기간, 할부기간, 생년월일 6자리가 그대로 노출돼 있다. 여기에 예약확인 여권정보, 현금영수증 정보 등까지 클릭할 수 있다.

(생략)

특히, 여권번호와 카드번호, 유효기간, 비밀번호 등은 개인 신용정보와 직접적으로 연관돼 있어 금전적 피해는 물론 2,3차 피해까지 발생할 수 있어 매우 위험하다. 더욱이 비행 출발시간, 도착시간, 비행편명 등의 정보까지 노출돼 있어 각종 위험에 노출될 수 있다. 무엇보다 이러한 중요 개인정보가 암호화 조치 없이 관리되고 있다는 것은 개인정보 보호법 안전성 확보조치 위반에 해당된다.

이와 관련 한 기업의 CISO는 “이번 사건은 이용자의 주요 정보가 모두 노출됐다는 점에서 프라이버시 침해의 심각성이 매우 크다고 볼 수 있다”며 “제3자에게 공개되는 경우, 신원 도용(identity theft)에 활용될 수 있는 정보가 버젓이 노출되어 있다. 또한, 이용자의 여행 경로가 노출되어 제3자에 의한 협박 및 갈취 등 2차 피해가 우려되는 문제점이 있다. 게다가 DB뿐 아니라 웹사이트에 파일의 형태(.html 포함)로 개인정보가 방치되고 있다는 점은 개인정보 관리가 얼마나 허술했는지 알 수 있다는 점에서 근본적인 개선이 필요하다”고 지적했다. (생략)

출처 : 보안뉴스 <http://www.boannews.com/media/view.asp?id=70904&kind=1>
김경애 기자 boan3@boannews.com

2018년 06월 01일

OO시, 탈북 직원 10여 명 신상정보 노출... “해당 직원 실수”

탈북민 출신의 OO시 산하기관 직원에 대한 신상 정보가 OO시 홈페이지에 넉 달 가까이 게재된 것으로 31일 드러났다. 탈북민의 개인정보 보안은 북한의 남은 가족의 신변에 직결되는 문제라 특히나 민감한 부분이다.

이날 OO시는 지난 1월 28일 OO교통공사가 시로 보낸 ‘북한이탈주민 채용현황 제출’ 문서가 지난 28일까지 시 홈페이지 ‘정보소통광장’에 공개됐다고 밝혔다. 정보소통광장은 OO시에서 생산·결제한 모든 문서를 시민에게 공개하는 사이트이다. 개인정보 등 민감한 정보를 담은 문서는 부분공개 또는 비공개 처리된다.

해당 문서에는 OO교통공사 측이 채용한 탈북민 출신 직원 10여 명의 이름과 성별, 생년월일, 채용일자, 정착기간 등 11가지 개인신상 정보가 포함됐고, 검색하면 누구든 볼 수 있는 ‘공개’ 상태였던 것으로 확인됐다.

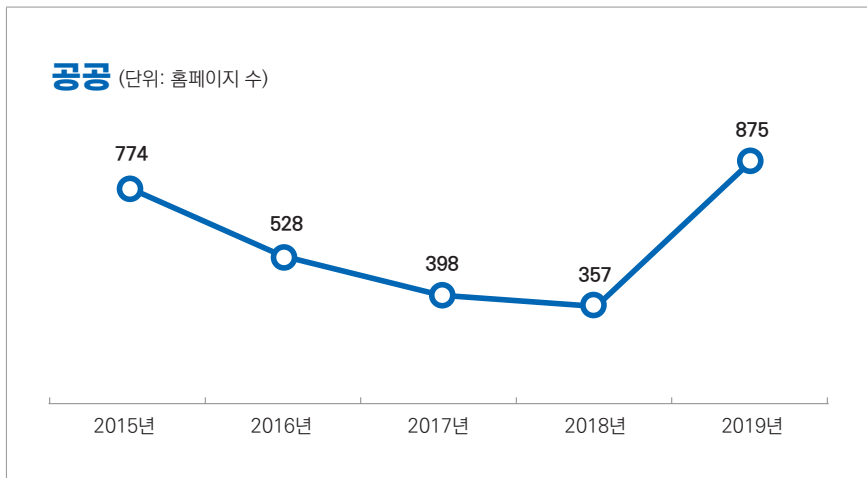
문서를 전부 공개로 설정해 올린 OO교통공사는 해당 문서를 OO시에 제출하는 과정에서 ‘비공개’로 설정해야 했으나 ‘담당자 실수’로 공개 처리됐다고 해명했다. 또 현재까지 이 문서가 30건 정도 조회된 것으로 나타나 비공개 처리했는데, 다행히 개인정보 노출에 따른 피해는 없었다고 덧붙였다.

OO시 관계자는 “산하기관이 결제한 문서의 공개 여부는 시스템상 해당 기관에서 설정하도록 돼 있다”며 “시 홈페이지 하루 이용자 수가 만 명에 달하는 만큼 개인정보 노출 방지를 위해 필터링 프로그램을 강화하겠다”고 밝혔다.

다. 숫자로 보는 개인정보 노출

공공부문에서의 개인정보 노출 탐지 추이를 살펴보면 개인정보 보호법 상 주민등록번호 등 주요 개인정보 처리에 대한 규제가 강화되고, 교육 등을 통해 개인정보 처리자의 인식이 제고됨에 따라 개인정보 노출 홈페이지 수는 지속적으로 감소세를 보이고 있다. 다만, 2019년에는 개인정보 탐지 유형을 고유식별정보 4종(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)에서 8종으로 확대(휴대전화번호, 계좌번호, 신용카드번호, 건강보험번호 추가)하고 이미지 파일 형태의 개인정보를 신규로 탐지함에 따라 노출 탐지 홈페이지 수가 875개로 다소 증가하였다.

그림 5 공공부문 개인정보 노출 탐지·삭제(홈페이지 수 기준)



정보통신서비스 제공자 등 민간 사업자의 경우 2013년도부터 개인정보 탐지 유형을 주민등록번호에서 개인정보 8종으로 확대(여권번호, 운전면허번호, 외국인등록번호, 휴대전화번호, 계좌번호, 신용카드번호, 건강보험번호 추가)하여 탐지하고 있다. 지속적인 시스템 고도화 등을 통해 2016년 이후 개인정보 노출 탐지 페이지 수가 증가하고 있으며 2019년에는 이미지 파일 형태의 개인정보를 신규로 탐지하는 등 12,615건의 노출 페이지를 삭제 하였다.

그림 6 민간부문 개인정보 노출 탐지·삭제(페이지 수 기준)

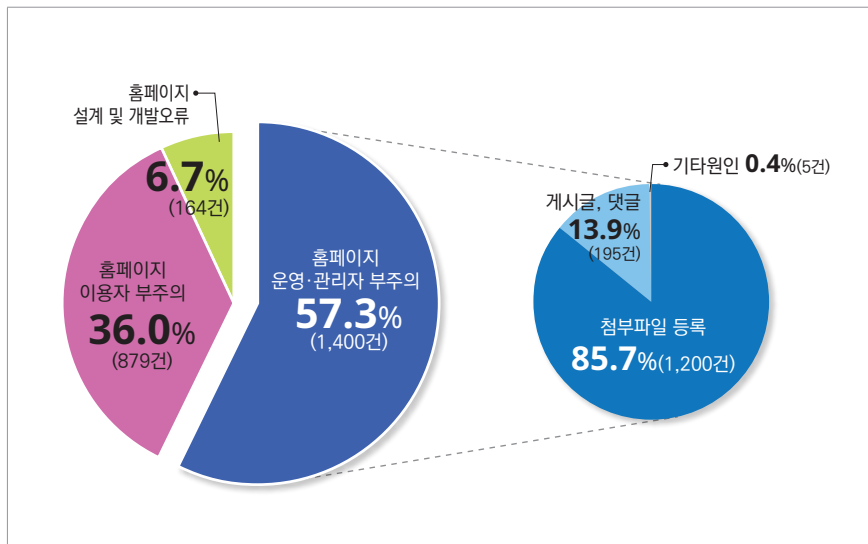


[그림7]은 최근 2년간('18년~'19년) 공공부문 홈페이지 개인정보 노출 원인을 분석한 결과로 개인정보 노출의 주된 원인으로는 '홈페이지 운영·관리자 부주의'가 총 57.3%(1,400건)로 약 과반수 이상을 차지했으며, 다음으로 '홈페이지 이용자 부주의'가 36.0%(879건)로 나타났다.

홈페이지 운영자 또는 관리자 부주의로 발생한 개인정보 노출의 경우에는 '개인정보가 포함된 첨부파일 등록'이 85.7%(1,200건)로 대부분을 차지했으며, '개인정보가 포함된 게시물 및 댓글'을 통한 노출도 13.9%(195건)로 분석되었다.

한편, 홈페이지 설계 및 개발 오류로 발생한 개인정보 노출은 총 6.7%(164건)로 상대적으로 적은 편이었으나, 대규모 개인정보 노출의 주된 원인이 되므로 홈페이지 설계·개발 단계부터 각별한 주의가 필요하다.

그림 7 공공부문 홈페이지 개인정보 노출 원인



**홈페이지
개인정보
노출방지
안내서**

개인정보 노출 원인 및 조치방안

1. 홈페이지 운영·관리자 부주의에 의한 노출
2. 이용자 부주의에 의한 개인정보 노출
3. 홈페이지 설계 및 개발 오류에 의한 노출
4. 검색엔진을 통한 개인정보 2차 노출

II

개인정보 노출 원인 및 조치방안

그림 8 개인정보 노출 원인 및 조치방안



1. 홈페이지 운영·관리자 부주의에 의한 노출

가. 개인정보가 포함된 게시물 및 댓글 게시

홈페이지 운영자 또는 관리자는 홈페이지 내 공지사항 등 게시판의 게시물, 댓글을 통해 개인정보가 인터넷에 노출되지 않도록 해야 한다.

노출사례 ① - 게시물에 개인정보 노출

G지원센터는 지역 내 기업들에게 각종 지원정보 및 상담 서비스를 운영하고 있다. 또한 기업의 신기술에 대해서 지정하고 고시하는 역할도 하고 있다. G지원센터의 관리자가 B기업의 신기술 관련 내용을 고시하는 과정에서 신기술개발자의 개인정보(이름, 주민등록번호, 주소)를 노출하였다.

그림 9 공지사항에 개인정보를 포함하여 게시

○ 신기술 보호기간 : 지정고시일로부터 3년

나. 신기술을 보유·개발한 기업(공동합치기술(기술))

○ 지정번호 : 제48호

○ 신기술개발자

- 회사명 : 서울(주)A
- 대표자 : 김(주)
- 법인주민등록번호 : 110111-111111, 330505-111111
- 주 소 : 서울특별시 강남구 테헤란로 123, 서울특별시 강남구 테헤란로 123

○ 신기술 내용 및 범위

- 신기술명 : 신기술(주)A 공동합치기술

○ 신기술 보호기간 : 지정고시일로부터 3년

다음글	다음(주)A 신기술개발자명상계제(변경)
이전글	신기술(주)A 기술개발 및 공동합치기술 상행함 전부개발됨

조치방법

상기 두 사례는 공지사항에 신기술 고시 및 정보주체의 민원을 해결하는 과정에서 홈페이지 운영·관리자 부주의로 개인정보가 노출된 건이다.

홈페이지 운영·관리자는 게시물 및 댓글 작성 시 ▲ 마스킹 등의 방법을 통해 최소한의 개인정보를 기재 ▲ 가능한 경우 개인정보 차단 소프트웨어를 통해 개인정보 포함 여부 사전 탐지 ▲ 부득이 개인정보를 적시해야 하는 경우 해당 게시물 및 댓글을 비공개로 전환하도록 해야 한다.

그림 11 게시판에 비공개 게시판으로 운영



나. 개인정보가 포함된 첨부파일 게시

홈페이지 운영자 또는 관리자는 개인정보가 포함된 첨부파일을 게시판에 게시할 경우, 불특정 다수에게 개인정보가 공개되지 않도록 비공개 게시판에 첨부파일을 게시하여야 한다.

특히 엑셀(Excel) 파일은 일정한 서식(행과 열)에 대량 정보를 저장하도록 고안되어 암호화를 하지 않고 공개 시 대량 노출로 이어질 가능성이 매우 높아 각별한 주의가 필요하다.

첨부 파일 종류에 따른 개인정보 노출 유형은 다음 [표 1]와 같다.

표 1 파일 유형 및 노출 사례

파일 유형	노출 사례
엑셀(.xlsx 등)	[숨기기] 기능에 의해 개인정보가 노출
	시트 보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보가 노출
	함수 치환 후 원본 내용 미삭제로 인해 개인정보가 노출
	[메모] 기능으로 개인정보가 노출
	배경색과 같은 글자색으로 개인정보를 작성하여 노출
	OLE(Object Linking and Embedding) 객체 연결로 인한 개인정보 노출
	외부 파일 참조 기능으로 인한 개인정보 노출
문서(.hwp .docx 등)	문서 파일에 개인정보가 노출
이미지(.jpg .png .pdf 등)	이미지 파일에 개인정보가 노출

노출사례 ① - 엑셀파일(.xlsx 등)에 의한 개인정보 노출

A시는 대표홈페이지 내 정보공개 게시판을 통해 법률에 따라 공개 의무가 있는 업무관련 자료를 업로드 하고 있다. 종합민원실 담당인 B씨는 관내 「부동산중개업 등록 및 폐업 현황」 엑셀 파일을 공개 게시판에 업로드 하면서 개인정보를 마스킹 또는 삭제 처리하지 않아 다수의 개인정보(이름, 주민등록번호, 소재지, 연락처 등)가 노출되었다.

그림 12 엑셀파일에 의한 개인정보 노출 사례

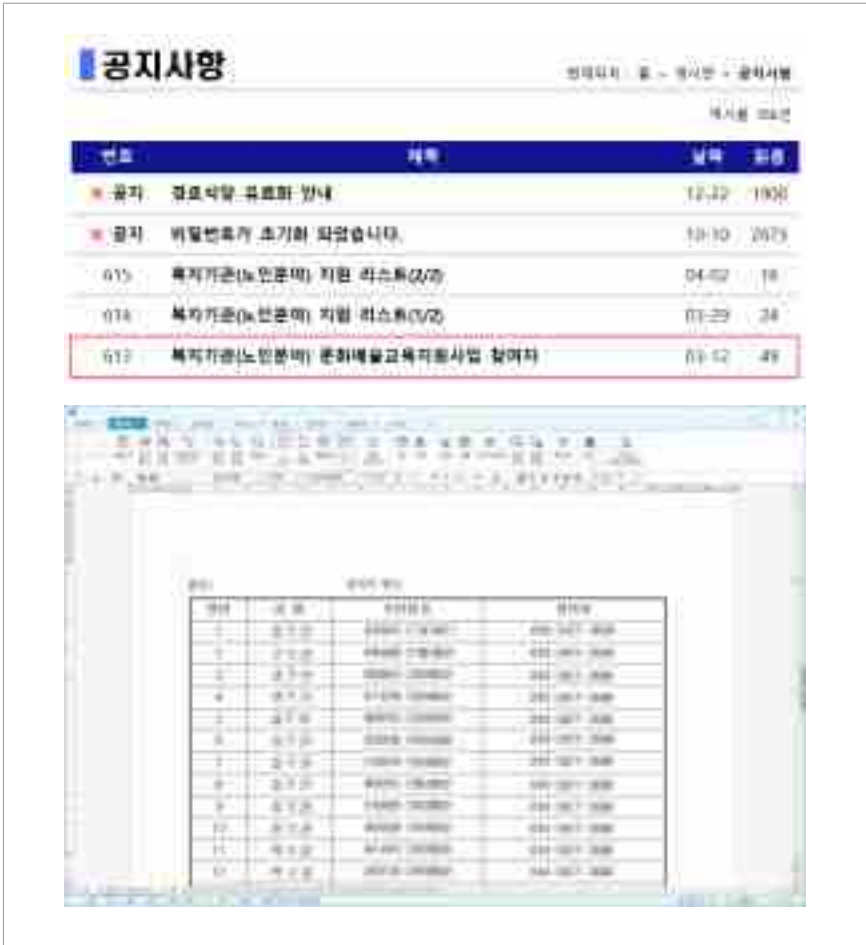
19.9.9	서울 수곡동 3남 및 인근 현황	서울 수곡동 3남 및 인근 현황(2019.9.9)	종합민원실
19.9.9	목격자대 신고 및 처리 현황	목격자대 신고 및 처리 현황(2019.9.9)	종합민원실
19.9.9	철도경찰청 수사팀 및 대령부	철도경찰청 수사팀 및 대령부(2019.9.9)	종합민원실
19.9.9	광안동제1차 아파트 화재현황 및 화재	광안동제1차 아파트 화재현황(2019.9.9)	종합민원실
19.9.9	부동산중개업 등록 및 폐업현황	부동산중개업 등록 및 폐업현황(4분기)	종합민원실

구분	이름	연락처	소재지	주요업무	주요사항	비고
1	김민준	010-1234-5678	서울 강남구	부동산중개업	2019.09.01	정상
2	이준호	010-2345-6789	서울 강남구	부동산중개업	2019.09.01	정상
3	박지민	010-3456-7890	서울 강남구	부동산중개업	2019.09.01	정상
4	정민준	010-4567-8901	서울 강남구	부동산중개업	2019.09.01	정상
5	최민준	010-5678-9012	서울 강남구	부동산중개업	2019.09.01	정상
6	한민준	010-6789-0123	서울 강남구	부동산중개업	2019.09.01	정상
7	정민준	010-7890-1234	서울 강남구	부동산중개업	2019.09.01	정상
8	최민준	010-8901-2345	서울 강남구	부동산중개업	2019.09.01	정상
9	한민준	010-9012-3456	서울 강남구	부동산중개업	2019.09.01	정상
10	정민준	010-0123-4567	서울 강남구	부동산중개업	2019.09.01	정상

노출사례 ② - 문서파일(hwp, .docx 등)을 통한 개인정보 노출

A복지관은 65세 이상 연장자를 대상으로 문화예술교육을 지원하고 있다. 분기별로 온·오프라인을 통해 신청자 접수를 받아, 참여자 명단을 홈페이지를 통해 공개하고 있다. 담당자 B씨는 문화예술교육지원사업 참여자 명단이 포함된 문서파일의 개인정보를 마스킹하지 않고 공지사항 게시판에 업로드하여 해당 개인정보(성명, 주민등록번호, 연락처)가 노출되었다.

그림 13 문서파일에 의한 개인정보 노출 사례



노출사례 ③ - 이미지 파일(.jpg .png .pdf 등)을 통한 개인정보 노출

A씨는 B여행사를 통해 항공권과 숙소를 예약했다. A씨는 예약인원 추가를 위해 여권사본(스캔본)을 여행사 담당자에게 메일로 보냈다. 하지만 업무담당자가 예약자 확인을 위해 홈페이지 공개 게시판에 여권사본 이미지 파일을 등록하면서 해당 개인정보(이름, 여권번호, 생년월일 등)가 노출되었다.

그림 14 이미지 파일에 의한 개인정보 노출 사례



조치방법

상기 사례는 홈페이지 운영·관리자가 민원인 응대 과정 등에서 개인정보가 포함된 파일을 업로드하면서 해당 개인정보가 노출된 사례이다.

홈페이지 운영·관리자는 첨부파일 업로드 시 ▲ 첨부파일 내 개인정보 마스킹 ▲ 첨부파일이 공개되지 않도록 접근 제어 ▲ 가능한 경우 개인정보 차단 소프트웨어를 통해 첨부파일 내 개인정보 포함 여부 사전 탐지 등의 조치를 취해 개인정보가 노출되지 않도록 해야 한다.

홈페이지 운영·관리자는 첨부파일 업로드 전에 해당파일 내 개인정보가 존재하는지 확인해야 하며, 공개된 게시판에 첨부파일을 업로드 해야 하는 경우 마스킹 처리 등을 통해 개인정보가 식별되지 않도록 조치해야 한다.

엑셀이나 한글 및 텍스트 기반의 PDF 파일은 검색 기능을 통해 개인정보가 포함되어 있는지 확인 가능하지만 이미지는 검색 기능을 통해 확인이 어려우므로 PDF 파일 생성 전 개인정보 포함 여부를 반드시 육안으로 확인 후, 마스킹 처리하여 PDF 파일로 변환하여야 한다.

그림 15 이미지 마스킹 처리 예시



이미지 첨부파일(.jpg .png .pdf 등)이 노출되었을 경우에는 해당 게시글을 비공개로 전환한 후에 첨부파일을 먼저 삭제하고, 이미지를 편집할 수 있는 소프트웨어(그림판 등)를 사용하여 개인정보를 마스킹 처리한 후 재등록하도록 해야 한다.

이미지 파일 및 이미지형 PDF 파일 등을 마스킹 처리할 경우, 도형 등 ‘객체’를 활용하여 마스킹 처리하지 않도록 주의해야 한다. ‘객체’를 이용해 개인정보를 마스킹할 경우 추후 객체 분리가 가능하여 개인정보가 노출될 수 있어, 이미지 상 개인정보를 완전히 삭제하거나 원본으로 복원이 불가능하도록 이미지 편집 소프트웨어에서 제공하는 마스킹 기능 등을 활용하여야 한다.

엑셀이나 한글 등 편집이 가능한 형태의 첨부파일을 게시판에 게시할 경우 소프트웨어의 다양한 부가기능을 사용하여 개인정보가 노출될 수 있다. 이용자 공지 등을 위한 용도의 공개용 파일은 PDF로 변환하여 활용하는 것을 권장한다.

그림 16 엑셀 및 한글 파일 PDF 변환 예시



NOTE!

엑셀파일의 경우에는 다양한 부가기능을 통해 개인정보가 숨겨져 있는 경우가 있으니
‘[여기서, 잠깐] 개인정보 노출의 원인이 되는 엑셀 기능 알아두기’를 참고하시기 바랍니다.

여기서, 잠깐!

개인정보 노출의 원인이 되는 엑셀 기능 알아두기

1) 숨기기

엑셀의 [숨기기(H)]란 행/열 또는 시트를 숨기기 처리하여 현재 화면에서 보이지 않게 처리하는 기능이다. 시트 내에서 숨기고 싶은 행/열에 마우스 우클릭 시 나타나는 메뉴에서 [숨기기(H)]를 클릭하는 경우, 해당 행/열이 숨김처리가 되고 숨김처리된 행/열은 보이지 않는 상태가 된다.

그림 17 숨기기 메뉴



그림 18 숨기기 기능 사용 후

D	F	G	H
2015년	2017년	2018년	2019년

숨기기 기능 사용 시 E열이 위 그림과 같이 보이지 않게 된다.

숨겨진 행/열은 [숨기기 취소(U)] 기능을 이용해 나타나게 할 수 있다. 숨겨진 열인 E열의 양옆에 있는 열(D~F)을 드래그한 후 우클릭 시 나타나는 메뉴에서 [숨기기 취소(U)]를 선택해 숨겨진 열을 숨김 취소할 수 있다.

그림 19 숨기기 취소 메뉴

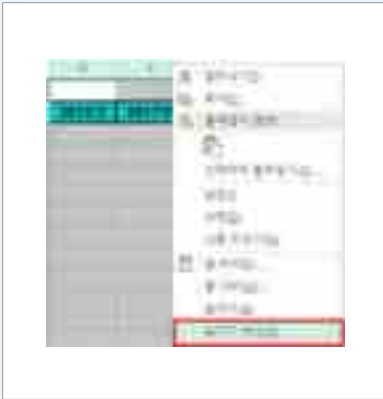


그림 20 숨기기 취소 기능 사용 후



개인정보가 포함된 행/열 또는 시트를 [숨기기] 처리한 파일을 열었을 때에는 개인정보가 바로 보이지 않지만 행/열 또는 시트 [숨기기 취소]를 할 경우 개인정보가 나타나기 때문에 개인정보 노출이 발생하게 된다.

노출예시

엑셀의 숨기기 기능을 잘못 활용하여 개인정보 노출이 발생하는 경우이다. 개인정보가 있는 셀을 행/열 또는 시트 [숨기기] 처리 후 업로드 하여 현재 보이지 않는 상태이지만, 숨겨진 정보는 삭제된 것이 아니라 그대로 남아있어 개인정보 노출이 발생하게 된다.

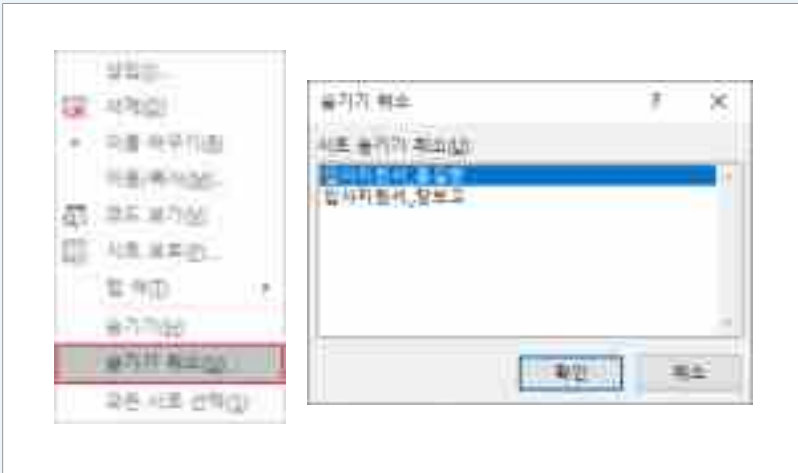
그림 21 숨기기 기능을 통한 개인정보 노출 예시



조치방법

홈페이지 운영·관리자는 첨부파일 업로드 전 엑셀 파일에서 행/열 또는 시트 [숨기기 취소] 기능으로 숨겨진 개인정보가 있는지 확인 후 개인정보가 존재할 경우 삭제하거나 식별할 수 없도록 마스킹 처리 및 업로드 해야 한다.

그림 22 숨기기 처리된 개인정보 확인



2) 시트 보호

엑셀의 [시트 보호]란 특정 워크시트에 대해 접근권한을 설정하여, 접근권한이 없는 자의 데이터 수정을 방지하는 기능이다. (MS OFFICE 2016 버전의 경우)파일 → 정보 메뉴 → 통합문서 보호 → 현재 시트 보호(P) 메뉴를 클릭 시 사용할 수 있다.

그림 23 시트 보호 메뉴



그림 24 시트 보호 설정



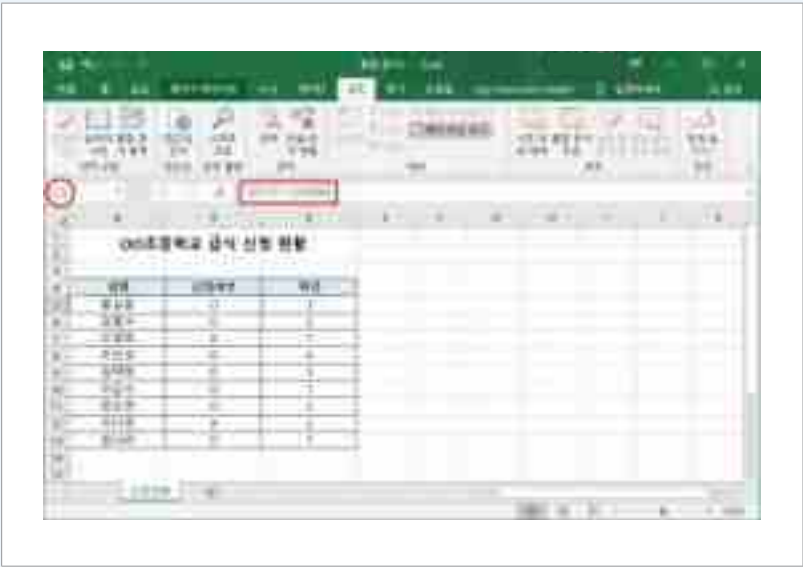
노출예시

일부 사용자는 엑셀 내 개인정보가 포함된 경우 문서 전체를 암호화하는 대신, 해당 행 또는 열을 숨기기 처리하고 숨기기 취소가 안 되도록 시트 보호기능을 설정한다. 하지만 시트 보호기능을 설정하더라도 데이터가 암호화되지 않으며, 찾기 및 바꾸기[Ctrl+F] 기능을 통해 데이터 검색이 가능하여 개인정보가 노출되게 된다.

그림 25 시트 보호로 개인정보가 보호되지 않는 예시(1)



그림 26 시트 보호로 개인정보가 보호되지 않는 예시(2)



조치방법

파일 사용자가 시트 보호 비밀번호를 알지 못할 경우 원칙적으로 숨겨진 행/열의 정보 확인이 불가능하다. 하지만 찾기 및 바꾸기[Ctrl+F] 기능, 개인정보 탐지 소프트웨어 또는 검색엔진 등에 의해 보호된 개인정보가 노출될 수 있으므로, 시트 보호기능이 적용된 시트에 개인정보를 포함해서는 안 된다.

3) 치환 함수

엑셀 함수를 이용하면 특정 명령어를 사용하여 방대한 양의 작업을 손쉽게 처리할 수 있다. 그 중 REPLACE, SUBSTITUTE, LEFT 함수 등은 텍스트를 특정 문자열로 바꾸는 기능으로 개인정보(휴대전화번호, 주민등록번호, 운전면허번호 등)를 마스킹 처리할 때 사용할 수 있다.

표 2 REPLACE, SUBSTITUTE, LEFT 함수 사용 예시

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

해당 함수를 사용하여 개인정보를 마스킹할 경우 결과값은 마스킹 처리(*****)되어 보이지만, 원본 데이터는 참조되어 남아있게 된다. 결국 육안으로는 마스킹 처리되었지만 실제로는 해당 정보가 엑셀 내 남아 있게 되는 것이다.

노출예시

개인정보가 포함된 셀을 REPLACE 등의 함수를 이용하여 마스킹 처리(D열) 했지만 원본(I열)은 마스킹 되지 않고 남아있다. 엑셀 내 함수를 이용하여 마스킹 처리 후 원본을 삭제하지 않아 개인정보가 노출된 사례이다.

그림 27 함수 치환 기능을 통한 개인정보 노출 예시

[illegible]

그림 28 함수 치환 후 값 붙여넣기 및 삭제



4) 메모

엑셀의 [메모]는 개별 셀에 주석을 추가하여 추가 설명 등을 제공할 수 있는 기능이며 메모가 있는 셀의 모서리에는 빨간색 표식이 나타난다. 메모가 있는 셀의 빨간색 표식에 마우스를 놓으면 해당 메모가 표시된다. 메모 기능은 메모를 추가하고 싶은 셀에 마우스 우클릭 후 나타나는 메뉴에서 [메모 삽입(M)]을 클릭하여 설정할 수 있다.

그림 29 메모 삽입 메뉴



그림 30 메모 삽입 후 화면



노출예시

업무상 편의를 위해 마스킹 처리된 개인정보의 원본을 [메모]에 작성한 경우이다. [메모]에 개인정보 작성 시, 평소 육안으로는 보이지 않지만 메모의 빨간색 표식에 마우스 커서를 올려놓거나 [메모 표시] 기능을 사용할 경우 개인정보가 노출된다.

그림 31 메모 기능을 통한 개인정보 노출 예시



The screenshot shows a table with 5 columns: NO, 성명, 주민등록번호, and two unlabeled columns. A red box highlights the '메모' (Memo) field in the third row, which contains the text '주민등록번호: 989812-11111111'. The table data is as follows:

NO	성명	주민등록번호			제입액
1	김+철	740010-1*****			1,000,000
2	김+미	001000-1*****			1,500,000
3	김+길	550000-2*****			3,000,000
4	마+시	710700-2*****	14		1,400,000
5	박+호	401210-2*****	14		1,400,000
6	권+동	500500-1*****	18		1,800,000
7	고+필	400607-1*****	22		2,200,000

조치방법

숨겨진 메모는 [메모 표시] 기능을 통해 언제든지 내용을 다시 확인할 수 있으므로 개인정보가 포함되어 있는 메모는 삭제해야 한다.

5) 글자색과 배경색이 같은 경우

파일 내 개인정보의 글자색과 배경색이 같아 개인정보가 없는 것처럼 보이는 경우이다. 육안으로는 보이지 않지만, 검색이나 드래그를 통해 개인정보를 확인할 수 있다.

노출예시

다음은 주민등록번호를 배경색과 같은 글자색(흰색)으로 작성하여, 육안으로 확인할 수 없었던 경우이다.

그림 32 배경색과 같은 색상으로 글자색을 지정하여 개인정보가 노출된 예시

성명	주민등록번호	생년월일	전화번호
김민준	702012-1010000000	2000-12-01	010-1234-5678
김민준	702012-1010000000	2000-12-01	010-1234-5678
김민준	702012-1010000000	2000-12-01	010-1234-5678
김민준	702012-1010000000	2000-12-01	010-1234-5678
김민준	702012-1010000000	2000-12-01	010-1234-5678
김민준	702012-1010000000	2000-12-01	010-1234-5678

조치방법

엑셀 파일을 홈페이지에 업로드 하는 경우에는 반드시 전체 셀을 선택 후 셀 배경색을 채우기 없음 및 글자색을 설정하여 숨겨진 개인정보가 있는지 확인해야 한다.

그림 33 셀 배경색 채우기 없음 설정



그림 34 글자색 자동 설정



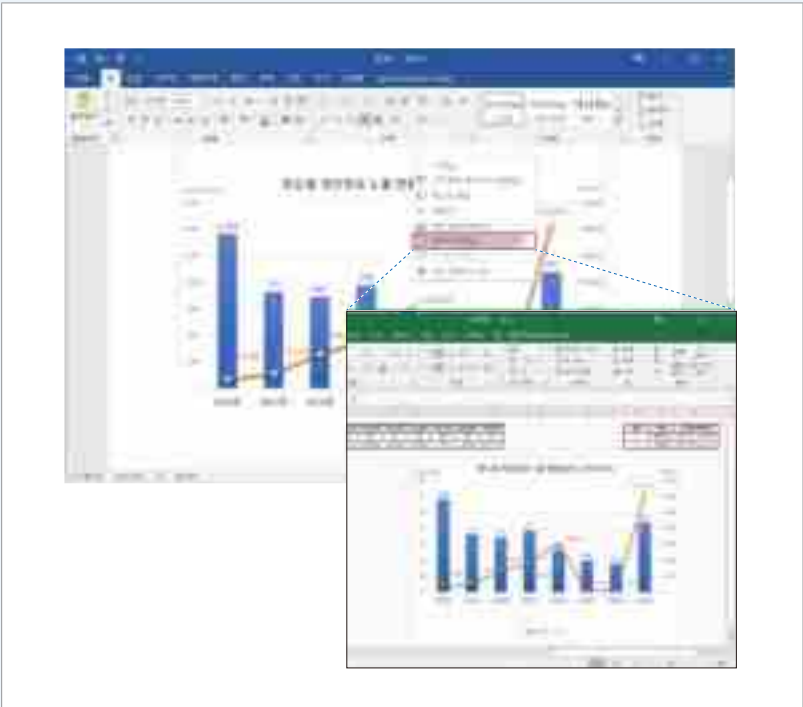
6) OLE 객체

OLE(Object Linking and Embedding)는 마이크로소프트에서 개발한 ‘통합문서’의 표준을 뜻한다. 응용 프로그램이 서로 호환되어 다른 응용 프로그램에서 작성한 그림이나 표, 차트, 비디오 등과 같은 데이터의 정보를 연결시켜 주는 기능이다.

노출예시

MS WORD 프로그램을 이용해 보고서 작성 중 엑셀에서 만든 차트를 OLE 객체 연결하여 사용하였다. 차트 내용 편집을 위해 MS WORD의 [데이터 편집] 기능을 사용하였고 연결된 엑셀에 저장되어 있던 개인정보가 노출되었다.

그림 35 OLE 객체에 의한 개인정보 노출 예시



조치방법

OLE 객체는 서로 다른 응용 프로그램에서 작성한 자료(차트, 이미지 등)를 연결하여 해당 응용 프로그램에서 사용하는 기능으로 다른 프로그램에서 작성한 내용이 함께 보여 질 수 있어, 외부 링크(파일연결)를 해제하고 사용하거나 OLE 객체에 포함된 엑셀시트의 개인정보를 삭제 또는 마스킹 처리해야 한다. (MS WORD 2016 버전의 경우) [파일 → 정보 → 파일 연결 편집 → 연결 끊기] 기능을 통해 다른 파일의 연결을 해제할 수 있다.

그림 36 OLE 객체에 의한 개인정보 노출 조치방법(1)

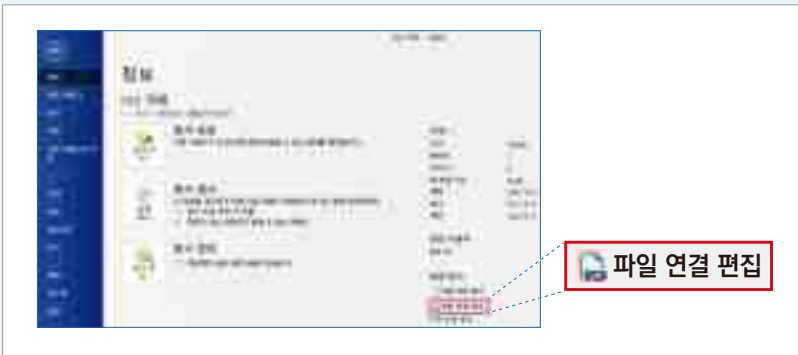
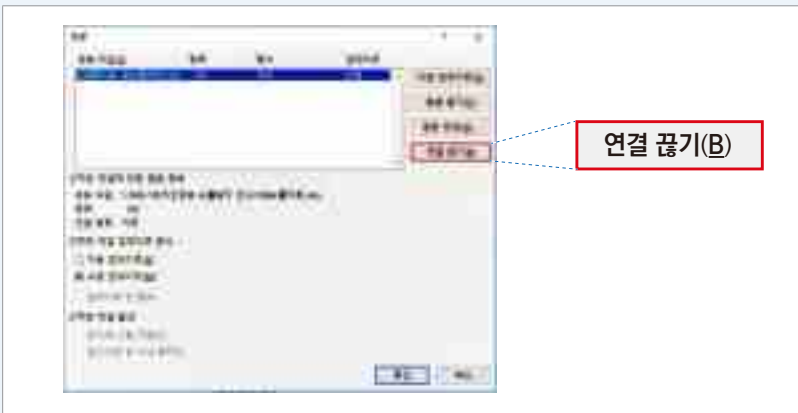


그림 37 OLE 객체에 의한 개인정보 노출 조치방법(2)



7) 외부 파일 참조

엑셀 함수(VLOOKUP 등) 활용 시, 외부 파일의 데이터를 연결하는 경우가 있다. 외부 파일을 연결할 경우 보다 손쉽게 외부 데이터를 가져와 쓸 수 있는 장점이 있지만 외부 파일에 저장된 모든 데이터가 엑셀에 저장되어 간단한 조작으로도 개인정보가 노출되는 사례가 발생하여 주의를 기울일 필요가 있다.

노출예시

외부 파일 참조 기능에 활용된 함수의 일부를 다른 함수 창에 입력하여 외부 파일에 저장된 개인정보가 노출되었다. 이 엑셀 파일은 압축 소프트웨어를 통해 압축 해제할 경우 참조되었던 파일의 개인정보가 나타났으며, 개인정보 탐지 소프트웨어를 통한 검사에서도 개인정보 노출 확인이 가능하였다.

그림 38 외부 파일 참조 함수를 이용한 개인정보 노출 예시

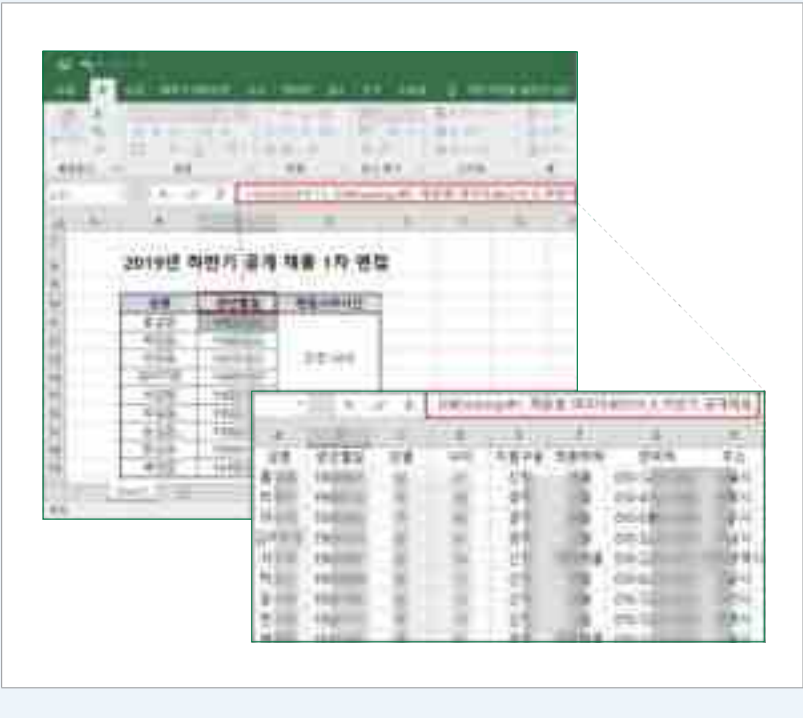
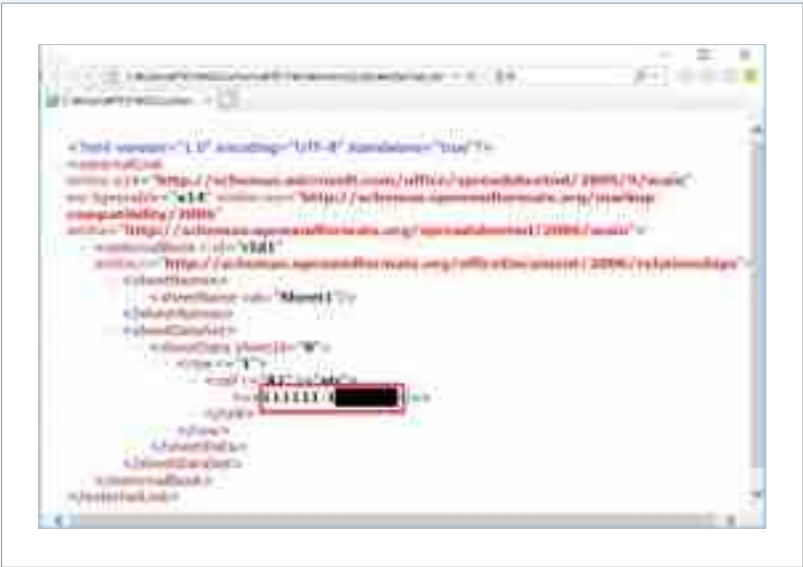


그림 39 외부 파일 참조 엑셀 파일 압축 해제 예시



그림 40 엑셀 파일 압축 해제를 통한 개인정보 노출 예시



조치방법

외부 파일 참조는 참조된 파일의 모든 데이터를 볼 수 있으므로 외부 파일 참조 수식을 활용한 행/열의 함수 삭제 및 ‘외부 연결 값 저장’ 옵션을 해제하여야 한다. 외부 파일을 참조 시, 외부 파일 참조 수식을 활용한 행/열을 ‘값 붙여넣기’하여 함수를 삭제하고, (MS OFFICE 2016 버전의 경우) 파일 → 옵션 → 고급 → 외부 연결값 저장 체크 박스를 해제하여야 한다. 추가 조치로 엑셀 수식 메뉴의 ‘이름관리자’ 기능 내 리스트를 삭제하고, 가능한 경우 개인정보 탐지 소프트웨어 등을 활용하여 파일 내 개인정보 포함 여부를 점검하도록 권고한다.

그림 41 ‘외부 연결 값 저장’ 옵션 해제 및 탐지 소프트웨어 활용 예시



2. 이용자 부주의에 의한 개인정보 노출

가. 개인정보가 포함된 게시물 및 댓글 작성

홈페이지 운영자 또는 관리자는 이용자가 홈페이지 내 공지사항 등 게시판의 게시물, 댓글에 개인정보를 기재할 경우 해당 개인정보가 인터넷에 노출되지 않도록 관리해야 한다.

노출사례 ① - 게시물에 개인정보 노출

신혼여행을 계획 중인 A씨는 마일리지로 좌석 업그레이드 서비스를 신청하기 위해 여권번호가 포함된 문의 글을 항공사 고객센터 게시판에 공개글로 작성하면서 개인정보가 노출되었다.

그림42 홈페이지 이용자의 게시물에 개인정보가 노출된 사례



노출사례 ② - 이용자 문의 댓글에 개인정보 노출

개인사업자인 A씨는 P사 홈페이지에서 물품을 구매하면서 세금계산서 발급을 요청하였다. 뒤늦게 세금계산서가 발급되지 않았다는 사실을 알게 된 A씨는 P사 홈페이지에 댓글로 세금계산서 발급을 요청하면서 개인정보(성명, 주민등록번호, 연락처)가 노출되었다.

그림 43 댓글에 의한 개인정보 노출 사례



조치방법

상기 두 사례는 홈페이지 이용자가 게시판 및 댓글을 통해 문의하는 과정에서 홈페이지 이용자의 부주의로 개인정보가 노출된 건이다.

홈페이지 운영·관리자는 홈페이지 운영 중 이용자 부주의에 의한 개인정보 노출이 발생하지 않도록 ▲ 게시물 비공개 전환 ▲ 게시물 삭제 ▲ 개인정보를 입력하지 않도록 안내 ▲ 비공개 게시판 운영 등의 조치를 취하고 관리해야 한다.

홈페이지 이용자가 작성한 게시물에 개인정보가 포함되어 있을 경우, 게시물을 비공개 전환하여 개인정보가 노출되지 않도록 임시조치하고, 해당 게시물을 삭제하거나 개인정보를 123456-1*****와 같이 마스킹 처리 한 후 재등록해야 한다.

이 후 게시글 작성 시 작성 글에 개인정보를 포함하지 않도록 공지사항 또는 안내 문구를 이용하여 작성자에게 안내해야 한다.

나. 개인정보가 포함된 첨부파일 게시

홈페이지 운영자 또는 관리자는 이용자가 개인정보가 포함된 첨부파일을 등록할 경우 비공개 게시판에 첨부파일을 게시할 수 있도록 관리해야 한다.

특히 엑셀 파일은 일정한 서식(행과 열)에 정보를 대량으로 저장하도록 고안되어 암호화를 하지 않고 공개 시 대량 노출로 이어질 가능성이 높아 각별한 주의가 필요하다.

노출사례 ① - 문서파일(.hwp, .docx 등)을 통한 개인정보 노출

A지자체는 정상운행이 가능한 오래된 경유자동차를 조기 폐차할 경우 보조금을 지원하고 있다. 이 사업을 알게 된 C씨는 노후차량 조기폐차 보조금을 지급받기 위해 “조기폐차 보조금 지급청구서”를 작성하여 A지자체 홈페이지에 게시하였다. 하지만 개인정보(성명, 주민등록번호, 주소, 휴대전화번호 등)가 기재된 지급청구서를 공개된 게시판에 업로드 하여 개인정보가 노출되었다.

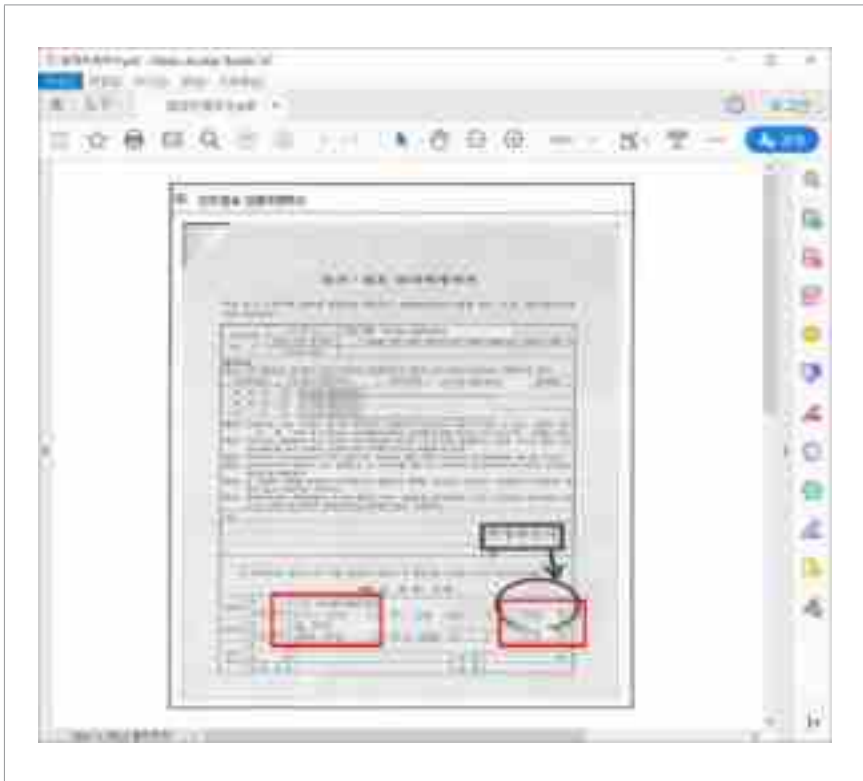
그림 46 문서파일을 통해 개인정보가 노출된 사례



노출사례 ② - 이미지 파일(.jpg, .png, .pdf 등)을 통한 개인정보 노출

주택재개발 사업을 진행 중인 A구청은 지역 주민 의견 수렴을 위해 홈페이지 내 민원 게시판을 운영하였다. 재개발사업 지역에서 상가를 운영하고 있는 C씨가 A구청에 민원을 제기하는 과정에서 상가·점포 임대차계약을 공개 게시판에 업로드 하여 개인정보(성명, 주민등록번호, 휴대전화번호, 주소 등)가 노출되었다.

그림 47 이미지형 PDF 파일에 의한 노출 사례



조치방법

상기 두 사례는 홈페이지 이용자의 부주의로 인해 개인정보가 포함된 첨부파일을 업로드하면서 개인정보가 노출된 경우이다.

홈페이지 운영·관리자는 이용자 부주의에 의한 개인정보 노출이 발생하면 ▲ 게시물 비공개 전환 ▲ 게시물 삭제 ▲ 개인정보를 입력하지 않도록 안내 ▲ 비공개 게시판 운영 등의 조치를 취해 개인정보가 노출되지 않도록 관리·감독해야 한다.

이용자가 업로드 한 첨부파일에 의해 개인정보 노출이 발생하면 홈페이지 운영·관리자는 해당 작성글을 삭제 후 이용자에게 개인정보가 포함되어 게시글을 삭제한 내용을 안내하거나, 해당 게시글을 신속히 비공개 처리하여 작성자와 홈페이지 운영·관리자만 열람할 수 있도록 조치해야 한다.

추가 조치로 공개 게시판에 글 작성 시 개인정보를 포함하지 않도록 공지사항 또는 안내 문구를 통해 작성자에게 안내해야 한다. 업무상 개인정보 입력이 불가피한 경우에는 해당 게시판을 비공개 게시판으로 운영하여 작성자와 홈페이지 운영·관리자만 글을 확인할 수 있도록 조치해야 한다.

그림 48 게시판 글 작성 시 노출 방지 안내 및 비공개 설정 기능 제공



3. 홈페이지 설계 및 개발 오류에 의한 노출

가. 관리자페이지 접근제어 미흡

홈페이지에 가입한 정보주체의 개인정보를 조회·변경·다운로드할 수 있는 관리자 페이지는 인가된 홈페이지 운영자 또는 관리자만 접속할 수 있도록 구축·운영되어야 한다. 정보주체의 개인정보를 처리할 수 있는 관리자페이지가 인터넷에 노출될 경우, 일반적인 개인정보 노출 사례와 달리 대량의 개인정보가 노출될 수 있으므로 각별한 주의가 필요하다.

노출사례

A기관은 B기관과 합병하면서 도메인을 기존의 '*.co.kr'에서 '*.com'으로 변경하고, 홈페이지를 새롭게 개편하는 등 서버 이전 작업을 하였다. 하지만 홈페이지 운영·관리자는 서버 이전 완료 후에도 기존 서버를 종료하지 않고 구 서버의 관리자페이지가 외부망에서도 접근 가능하도록 방치하였다. 또한, 개발자의 실수로 관리자페이지의 비밀번호 설정이 해제되어 A기관 이용자의 개인정보가 관리자페이지를 통해 대량 노출되었다.

그림 49 관리자페이지 접근제어 미흡으로 노출된 사례



조치방법

상기 사례는 서버 이전 작업을 하며 ① 구 시스템 방치 및 ② 관리자페이지에 대한 외부 접근제어 미흡, ③ 관리자페이지 로그인 비밀번호 미설정 등으로 인해 개인정보 노출이 발생한 것이다.

개인정보 보호법 제29조에 따라 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용해야 한다. 관리자페이지에 접속하는 경우도 개인정보처리시스템에 접속하는 것으로 인정되는 바, 상기 의무사항이 관리자페이지 접속 시에도 적용된다.

따라서 홈페이지 운영·관리자 및 개발자는 ▲ 홈페이지 개편 등으로 인한 시스템 이전 시, 구 시스템 즉각 종료 ▲ 관리자페이지를 정보통신망을 통해 외부에서 접속할 경우 안전한 접속수단 혹은 안전한 인증수단 마련 ▲ 관리자페이지에 대한 접속 권한 제한 ▲ 관리자페이지 접속 주소가 ~/admin, ~/administrator, ~/manager 등 예측하기 쉬운 주소가 아닌지 확인 ▲ 디폴트 비밀번호 및 쉬운 비밀번호 사용 지양 ▲ 정기적인 웹 취약점 점검 등의 사항을 준수해야 한다.

NOTE!

홈페이지별로 관리자페이지에 적용되어 있는 접근제어 조치가 상이할 수 있습니다.
자세한 사항은 **「여기서, 잠깐! 관리자페이지 안전하게 보호하기」**를 참고하시기 바랍니다.

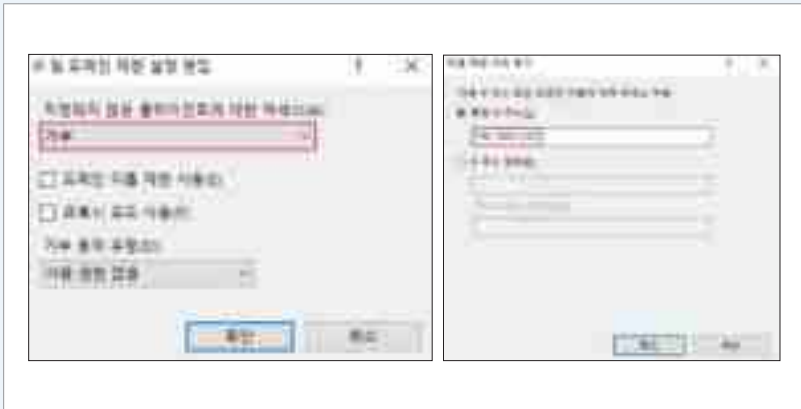
여기서, 잠깐!

관리자페이지 안전하게 보호하기

관리자페이지에서의 개인정보 노출을 방지하기 위해, 개인정보처리자는 외부에서 관리자페이지에 접속할 경우 안전한 접속수단 혹은 안전한 인증수단을 마련해야 한다. 전용선 및 가상사설망(VPN)을 통해 관리자페이지에 접속할 수 있도록 접근제어하거나, 휴대전화인증 및 공인인증서, OTP 등 추가 인증(2-Factor 인증)을 통해 접속할 수 있도록 해야 한다.

그림 50 OTP**그림 51** 휴대전화인증**그림 52** 공인인증서

관리자페이지에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다. 이 경우 해당 단말기(접속권한이 있는 IP를 부여받은 PC)가 다수의 사용자에게 의해 이용되거나, 네트워크를 통해 원격 접속되지 않도록 관리해야 하며, 관리자페이지에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출시도가 있었는지에 대해 탐지하고 대응해야 한다.

그림 53 관리자페이지 접속 권한 제한(특정 IP만 접속 허용)

또한 개인정보처리자는 관리되지 않는 사이트는 삭제·차단 조치해야 하며, 사용하는 사이트라 하더라도 방치된 게시판 등이 존재한다면 즉각 삭제·차단 조치해야 한다. 홈페이지에 관리자페이지의 주소를 링크로 만들어서는 안 되며, 관리자페이지의 주소를 쉽게 추측 가능한 주소로 사용하지 않아야 한다.

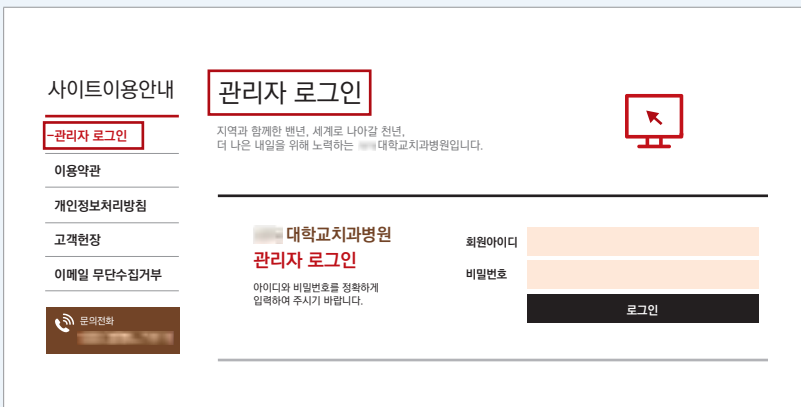
그림 54 관리자페이지의 링크 예시

그림 55 추측 가능한 관리자페이지 주소 예시

개인정보처리자는 디폴트 비밀번호 및 쉬운 비밀번호를 사용하지 않도록 해야 하며, 주기적으로 이를 점검해야 한다.

그림 56 주기적인 비밀번호 변경 예시

개인정보처리자는 인터넷 홈페이지의 설계·개발 오류 또는 홈페이지 운영·관리자의 업무상 부주의 등으로 인터넷 검색 엔진을 통해 관리자 페이지가 노출되지 않도록 필요한 조치를 취해야 하며, 정기적으로 검색엔진에 노출되는지 점검해야 한다.

고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 노출되지 않도록 연 1회 이상 디렉터리 리스팅 취약점, 파라미터 변조 등 웹 취약점을 점검하고 필요한 보완조치를 하여야 하며, 고유식별정보를 처리하지 않는 개인정보처리자라 하더라도 개인정보 노출의 위험성을 줄이기 위하여 정기적으로 웹 취약점을 점검하도록 권고한다.

그림 57 디렉터리 리스팅 취약점 예시



※ 보다 자세한 조치 사항 및 취약점 점검 등에 활용 가능한 자료는 [부록 5] 참고자료(p.135) 참조

나. 홈페이지 접속경로(URL) 관련 오류

1) URL 내에 개인정보 포함

웹 전송방식은 변수명, 변수 값이 URL에 보이는 지 유무에 따라 GET 방식과 POST 방식으로 구분된다. POST 방식이 변수명, 변수 값이 URL에 노출되지 않아 보안에 강하지만, 성능 및 외부 링크 시 추가 개발 등의 이유로 GET 방식을 사용하는 경우가 있다. 홈페이지 개발자는 POST 방식을 사용하도록 하고, 부득이하게 GET 방식을 이용할 경우 URL 내 개인정보가 포함되지 않도록 해야 한다.

노출사례 ① - 홈페이지 접속경로(URL)에 개인정보 포함

H고등학교는 홈페이지를 통한 이력서 관리 서비스를 학생들에게 제공하고 있다. 해당 이력서 관리 서비스의 URL에 학생 주민등록번호가 구분 값으로 사용되면서 개인정보가 노출되었다.

그림 58 URL에 주민등록번호가 노출된 사례



2) URL 내 포함된 변수 값을 조작하여 타인의 개인정보 조회

게시물 조회 시 GET 방식을 이용하는 경우(게시물 내용 조회를 위한 게시물 번호를 URL을 통해 웹 서버로 전달) 설계 및 개발 오류로 변수 값 조작을 통해 타인의 비공개된 게시물까지 조회되는 문제가 발생할 수 있다.

따라서 웹 전송방식으로 GET 방식을 이용하는 홈페이지 개발자는 변수 값 조작을 통해 타인의 정보가 조회되지 않도록 해야 한다.

노출사례 ② - 접속경로(URL) 변경을 통한 타인의 개인정보 접근

대학생인 K씨는 이메일이 변경되어 해당 정보를 수정하기 위해 학사관리시스템에 접속하였다. K씨는 홈페이지 URL 내 파라미터로 자신의 학번이 사용되는 것을 확인하고, 호기심에 친구의 학번을 입력하자 친구의 개인정보(이메일, 주소, 연락처 등)를 수정할 수 있는 페이지가 출력되었다.

그림 59 URL값 변경 시 다른 회원의 정보가 노출된 사례



조치방법

상기 사례는 홈페이지 설계 및 개발 오류로 ① 홈페이지 전송방식으로 GET 방식 사용 ② URL 내 파라미터로 개인정보(주민등록번호 등)를 사용하여 개인정보 노출이 발생한 것이다.

홈페이지 접속경로(URL) 관련 오류로 인해 개인정보 노출이 발생하면 ▲ 사용자 자신의 정보만 조회 가능하도록 접근제어 ▲ 회원 구분 값 변경 ▲ 홈페이지 설계 변경(GET 방식에서 POST 방식으로) 등을 통해 개인정보 노출을 방지해야 한다.

접근권한 관리가 미흡한 경우 가입된 사용자들의 개인정보가 노출되어 해당 정보가 악용되는 피해가 발생할 수 있다. 이를 위해 회원정보가 조회 가능한 페이지는 이용자 본인만 확인할 수 있도록 인증 정보 확인 등의 방법으로 접근 통제해야 한다.

또한, 회원 구분 값으로 주민등록번호 등 개인정보를 이용해서는 안 되며, 웹 브라우저 주소 표시줄에 파라미터 값이 보이지 않도록 GET 방식 보다는 POST 방식을 사용하도록 해야 한다.

그림 60 URL에 개인정보가 노출된 경우 조치방법



여기서, 잠깐!

GET 방식과 POST 방식 알아보기

■ GET 방식

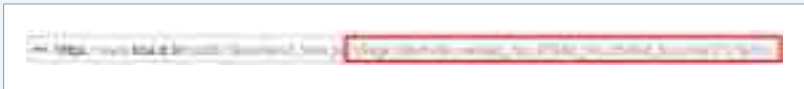
Form 태그 method 속성 값으로 GET을 지정할 경우 변수명, 변수 값이 URL 주소에 노출된다.

그림 61 GET 방식 예시



URL과 파라미터를 구분하기 위해 “?”를 구분자로 쓰며, 파라미터가 여러 개일 경우 “&”를 각 파라미터의 구분자로 사용한다. 즉, 구분자 “?” 뒤에 오는 값이 파라미터 값이다.

그림 62 GET 방식 파라미터 값 예시



URL 자체에 데이터를 포함시키기 때문에 URL 자체가 하나의 긴 문자열이다. 또한 HTTP 헤더에서 GET 방식으로 HTTP method 부분에 표시된다.

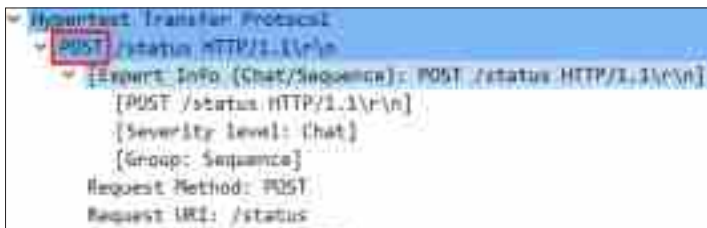
그림 63 GET 방식 HTTP 헤더



■ POST 방식

Form 태그 method 속성 값으로 POST를 지정할 경우 변수명, 변수 값이 URL 주소에 노출되지 않는다. GET 방식과는 다르게 길이의 제한이 없으며, 보안을 지킬 수 있다는 이점이 있다. 아래 그림과 같이 HTTP 헤더에서 POST 방식으로 HTTP method 부분에 표시된다.

그림 64 POST 방식 HTTP 헤더



```

Hypertext Transfer Protocol
  POST /status HTTP/1.1\r\n
    [Export Info (Chat/Sequence): POST /status HTTP/1.1\r\n]
    [POST /status HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: POST
    Request URI: /status
  
```

다. 홈페이지 소스코드 보안설정 미흡

정적홈페이지와 달리 동적홈페이지는 홈페이지 조회 시 매번 페이지를 새로 생성한다. 홈페이지 조회 시 WAS서버는 DB서버로부터 정보를 가져와 소스코드를 생성하고, 해당 소스코드가 웹 브라우저를 통해 이용자에게 보여진다. 문제는 개발자가 화면에서 보이는 것보다 더 많은 정보를 DB에서 가져오도록 개발하였다면, 화면에서 보이지 않는 개인정보 등이 소스코드에 포함된다. 따라서 개발 단계에서부터 불필요한 개인정보가 소스코드에 포함되지 않도록 주의하고, 부득이 개인정보가 소스코드에 포함되어야 한다면 반드시 필요한 정보(화면에서 보여지는 정보)만 소스코드 내에 포함되도록 개발해야 한다.

노출사례

노트북 중고 판매업체인 A사는 제품 홍보 등을 위해 홈페이지 내 특가 정보 게시판을 운영하고 있다. A사 직원인 H씨는 특가 정보 게시판에 노트북 특가 이벤트 관련 글을 게재하였다. 해당 게시글에는 개인정보가 표시되지 않지만, 홈페이지 소스코드 보안설정 미흡으로 해당 화면에서 마우스 오른쪽 클릭 후 [소스 보기]를 선택했을 때 작성자의 개인정보(주민등록번호)가 노출되었다.

그림 65 소스코드를 통해 개인정보가 노출된 사례



```
6. <td width="50%" valign="top">
7. <div style="border: 1px solid black; padding: 5px; width: 100%; text-align: center; margin-bottom: 10px;">
8. <div style="display: inline-block; width: 40%; text-align: left; vertical-align: top;">
9. <div style="display: inline-block; width: 40%; text-align: right; vertical-align: top;">
```

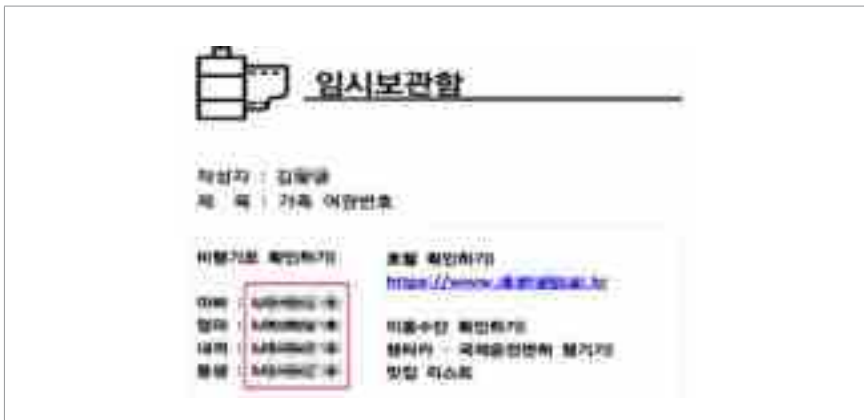

라. 임시 저장 페이지 미삭제

이용자 편의를 위해 임시 저장 페이지 기능 개발 시, 개발자는 이용자의 로그아웃 종료와 동시에 임시 저장했던 내용들이 모두 삭제되도록 해야 한다. 만일 삭제되지 않고 일정기간 보관하도록 해야 한다면, 임시 저장했던 내용이 로그인 등 인증 없이 인터넷에서 접근되지 않도록 해야 한다.

노출사례

K여행사는 홈페이지 내 고객 편의를 위해 고객 메모용으로 임시 저장 페이지 기능을 제공하였다. K여행사 회원인 A씨는 겨울 휴가로 가족 여행을 계획하면서, 여행사 홈페이지 내 임시보관함에 가족 구성원의 여권번호를 입력하였다. 그러나 K여행사의 임시보관함 페이지가 인터넷에 공개되면서, 해당 개인정보가 노출되었다.

그림 67 임시보관함에 저장된 개인정보 노출 사례



조치방법

상기 사례는 이용자 편의를 위해 제공된 임시 저장 페이지가 공개되면서 개인정보가 노출된 것이다.

홈페이지 개발자는 임시 저장 페이지에서 개인정보가 노출되지 않도록 ▲ 게시물 작성 완료 및 작성 취소 시 저장된 임시 저장 페이지 즉시 삭제 ▲ 일정기간이 경과된 임시 저장 페이지 자동 삭제 등의 조치를 취해야 한다.

마. 디렉터리 리스팅 보안설정 미흡

디렉터리 리스팅이란 보안 취약점 중 하나로 웹 서버 설정 미숙 등으로 웹 브라우저를 통해 웹 서버의 디렉터리, 파일 목록이 노출되고, 열람 및 다운로드가 가능하게 된 상태를 말한다. 홈페이지 개발자는 디렉터리 리스팅이 발생하지 않도록 사용하고 있는 웹 서버 등의 설정을 해야 한다.

특히 해당 유형에서는 웹 서버 내 모든 파일이 인터넷에 무방비로 노출되어 개인정보 유출 사고로 이어질 수 있으므로 각별한 주의가 필요하다.

노출사례

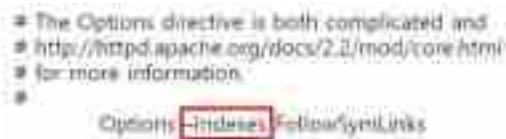
A협회 홈페이지에서 디렉터리 리스팅을 차단하지 않아 홈페이지 접속 시, 메인화면 대신 디렉터리 리스팅 화면이 출력되어 웹 서버 내 회원정보가 노출되었다.

조치방법

상기 사례는 홈페이지 설계 오류 중 디렉터리 리스팅 취약점에 의해 개인정보 노출이 발생한 건이다.

디렉터리 리스팅에 의해 개인정보 노출이 발생하면 ▲ 접근제어 설정 ▲ 디렉터리 설정 변경 등 해당 디렉터리를 외부에서 읽을 수 없도록 조치해야 한다. 웹 서버별 디렉터리 리스팅 취약점을 해결하는 방법은 다음과 같다.

- 1) Apache 1.x, 2.x : httpd.conf 파일에서 Indexes 설정을 제거



```
# The Options directive is both complicated and
# http://httpd.apache.org/docs/2.2/mod/core.html
# for more information.
#
Options Indexes FollowSymLinks
```

- 2) Tomcat : 웹 설정 파일(web.xml)에서 listing 파라미터(디렉터리 리스팅 설정)를 false로 변경



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


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



4) 윈도우즈 IIS(Internet Information Service) 환경

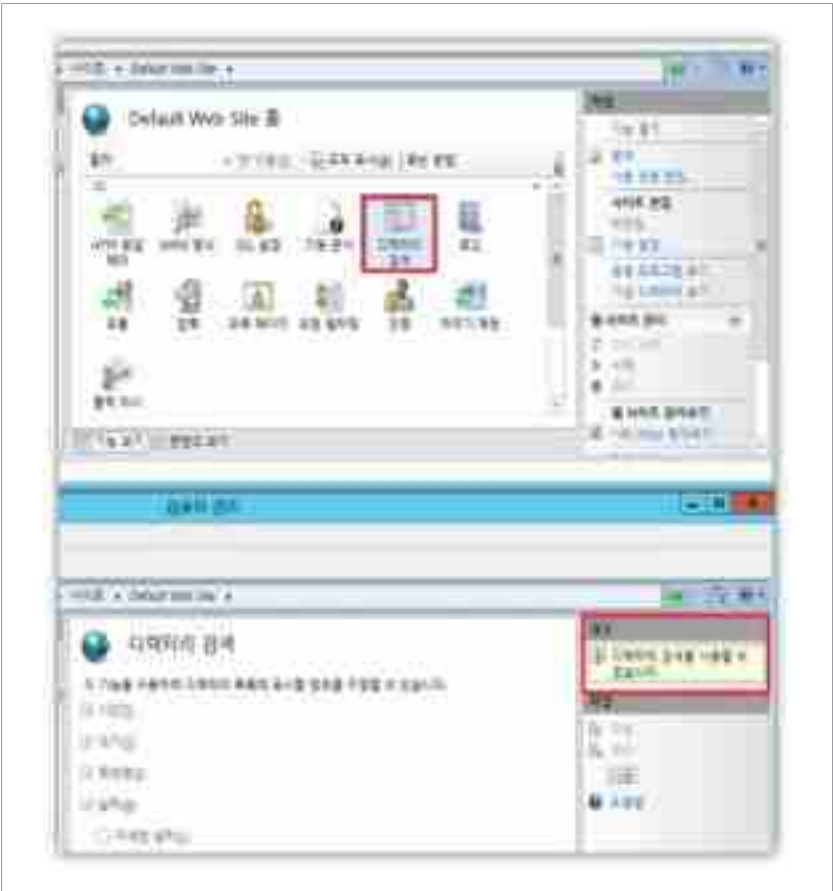
- ① IIS 6.x 이하 : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 웹사이트의 속성에서 디렉터리 검색 항목을 비활성화

그림 68 IIS 6.x 이하에서 디렉터리 리스팅 방지 설정



- ② IIS 7.x : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 웹사이트 홈 → 디렉터리 검색을 더블클릭 후 우측 작업창에서 사용 해제
- ③ IIS 8.x 및 IIS 10.x : 제어판 → 시스템 및 보안 → 관리도구 → IIS(인터넷 정보서비스) 관리자 → 사이트 → 기본 웹사이트 홈 → 디렉터리 검색을 더블클릭 후 우측 작업창에서 사용 해제

그림 69 IIS 7.x / 8.x / 10.x 에서 디렉터리 리스팅 방지 설정



4. 검색엔진을 통한 개인정보 2차 노출

가. 검색엔진의 이해

검색엔진이란 인터넷 상에서 자료를 쉽게 찾을 수 있도록 검색사이트에 구축된 기능이다. 검색엔진은 정보수집·정보가공·정보제공의 세 가지 기능으로 구성되는데 정보수집은 크롤러, 정보가공은 인덱서, 정보제공은 사용자 인터페이스가 담당한다. 검색엔진의 정보수집 단계에서 크롤러가 인터넷에 있는 웹사이트를 주기적으로 방문하여 각종 정보를 자동으로 수집하는데, 이 때 웹사이트의 일부 웹페이지가 검색엔진 내 일정기간 동안 보관된다. 가령 주민등록번호 등 개인정보를 포함한 웹페이지가 검색엔진에 수집될 경우 원 사이트에서 해당 웹페이지의 개인정보를 삭제 조치하더라도, 크롤러가 개인정보가 삭제 조치된 웹페이지를 재 수집하지 않는 동안 개인정보가 여전히 검색엔진에 검색될 수 있다. 따라서 홈페이지에 개인정보가 잠시라도 업로드 된 경우에는 반드시 해당 노출 내용이 검색엔진에 의해 수집되었는지를 확인하고 검색엔진에 남아 있는 개인정보를 삭제해야 한다.

노출사례

A협회는 화장품 제조사의 사업계획서 및 사업자등록증, 이력서 등을 관리하고 있다. A협회는 자체 개인정보 관리실태 점검 시 홈페이지 설계 상 오류로 직원 이력서가 노출된 사실을 인지하고 삭제 조치하였다. 하지만 삭제 조치된 직원 이력서가 검색엔진의 저장된 페이지에 남아있어, 이력서 내 개인정보가 검색엔진을 통해 2차 노출되었다.

그림 70 검색엔진을 통한 개인정보 2차 노출 예시



나. 검색엔진을 통한 2차 노출 방지 방안

우선 기관 홈페이지 내 개인정보가 인터넷에 노출되지 않도록 조치 완료 후, 검색엔진을 통한 2차 노출을 방지하기 위해 검색사이트에서 노출된 페이지의 URL 또는 노출된 값으로 검색을 수행해야 한다. 검색 결과, 조치 완료된 웹페이지가 검색사이트 캐시 페이지에 저장된 경우, 검색사이트에서 제공하고 있는 웹마스터 도구 또는 고객센터를 통하여 해당 캐시 페이지를 삭제해야 한다. 검색사이트별 캐시 페이지 삭제 요청 웹사이트는 다음과 같다.

표 3 검색사이트별 캐시 페이지 삭제 요청 주소

검색사이트	명칭	삭제 요청 주소
네이버(Naver)	웹 마스터 도구	https://help.naver.com/support/home.nhn
다음(Daum)	검색결과 제외	https://cs.daum.net/
구글(Google)	오래된 콘텐츠 삭제	https://www.google.com/webmasters/tools/removals
빙(BING)	콘텐츠 제거	https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d

1) 네이버(Naver)

인터넷에 노출된 개인정보가 네이버 검색엔진에 의해 2차 노출된 것을 발견하면, 아래와 같은 절차로 네이버 고객센터에 방문하여 삭제 조치를 수행한다.

그림 71 네이버 검색엔진 2차 노출 방지 조치 절차



① 네이버 고객센터 방문

네이버 고객센터를 방문하여 신고센터 → 유해 게시물 신고 메뉴를 클릭한다.

그림 72 네이버 고객센터 방문



② 네이버 게시물 신고 접수

게시물 신고 접수에서 신고하는 이유(개인정보 노출)를 선택한다.

그림 73 신고 접수 메뉴 선택 '개인정보 노출'



③ 노출되는 위치 선택

개인정보 노출 게시물이 어디에서 노출되고 있는지 선택한다.(네이버 검색결과)

그림 74 신고 접수 메뉴 선택 ‘네이버 검색결과’



④ 검색 제외 요청하기

개인정보 노출 게시물이 검색엔진에서 검색되지 않도록 ‘검색 제외 요청하기’ 메뉴를 선택한다.

그림 75 ‘검색 제외 요청하기’ 메뉴 선택



⑤ 게시물의 작성자 선택

개인정보가 노출된 게시물의 작성자를 선택한다.

그림 76 게시물의 작성자 선택



⑥ 게시물 상태 선택

검색 제외를 원하는 게시물의 상태를 선택한다. 원본 게시물이 삭제되지 않은 상태에서 캐시 페이지를 삭제할 경우, 추후 캐시 페이지로 재 노출될 수 있으므로 원본 게시물이 삭제된 후 캐시 페이지 삭제를 요청하는 것이 적절하다.

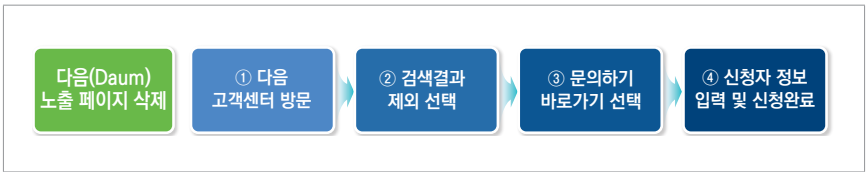
그림 77 원본 게시물의 삭제여부 선택



2) 다음(Daum)

인터넷에 노출된 개인정보가 다음 검색엔진에 의한 2차 노출된 것을 발견하면, 아래와 같은 절차로 다음 고객센터에 방문하여 삭제 조치를 수행한다.

그림 79 다음 검색엔진 2차 노출 방지 조치 절차



① 다음 고객센터 방문

다음 검색엔진의 고객센터에 접속하여 ‘검색’ 탭을 선택한다.

그림 80 다음 고객센터 화면에서 ‘검색’ 탭 선택



② 검색결과 제외 선택

고객센터 '검색' 탭에서 '검색결과 제외'를 선택한다.

그림 81 다음 고객센터 검색 탭에서 '검색결과 제외' 선택



③ 문의하기 바로가기 선택

검색결과 제외 탭에서 ‘개인정보가 포함된 게시글이 검색되는데 삭제할 수 있나요?’의 내용 확인 시 ‘문의하기 바로가기’ 링크를 통해 개인정보가 포함된 게시글을 삭제요청할 수 있다. 검색 URL, 키워드, 원문 URL, 원문게시물 제목, 삭제요청사유를 기입하여 삭제요청을 한다.

그림 82 ‘개인정보가 포함된 게시글 삭제’ 화면 선택



④ 신청자 정보 입력 및 신청완료

필수항목(이름, 답변 받을 이메일, 문의 분류, 제목, 내용)을 작성하여 개인정보 노출
삭제요청을 접수한다.

그림 83 개인정보 노출 삭제요청 접수

[illegible]

3) 구글(Google)

구글의 저장된 페이지에서 개인정보가 노출된 경우, 구글에서 제공하는 웹마스터 도구를 이용하여 검색엔진의 “저장된 페이지(캐시)”를 삭제요청 할 수 있다. 웹마스터 도구 삭제요청 절차를 자세히 살펴해보도록 한다.

그림 84 구글 검색엔진 2차 노출 방지 조치 절차



구글의 ‘오래된 콘텐츠 삭제’ 기능은 특정 사이트나 URL을 긴급 삭제하는 기능으로 웹사이트가 삭제되지 않더라도 구글 검색결과에서 임시 삭제된다. 임시적인 조치로 검색결과에서는 일정기간 동안만 보이지 않게 된다. 재노출될 가능성이 있으므로 웹사이트의 노출된 개인정보 삭제 후 ‘오래된 콘텐츠 삭제’ 기능을 이용해야 한다.

① 개인정보가 노출된 페이지 또는 파일 검색

검색엔진에서 노출된 페이지를 검색하여 노출된 페이지 URL 우측에 있는 아래 화살표를 클릭하여 저장된 페이지로 이동한다.

그림 85 노출된 페이지 URL 링크 옆 화살표 클릭



② 상단 캐시 URL 복사

남아있는 개인정보 확인 후 상단 캐시 URL을 복사한다.

그림 86 상단 캐시 URL 복사



③ 구글 로그인

구글의 오래된 콘텐츠 삭제 페이지(<https://www.google.com/webmasters/tools/removals>)로 이동 후 로그인한다.

그림 87 구글 로그인



④ 캐시 URL 주소 입력 및 분석

복사한 캐시 URL을 입력 후 삭제 요청한다.

그림 88 구글 오래된 콘텐츠 삭제 요청



그림 89 캐시 URL 분석



⑤ 콘텐츠 삭제 여부 선택

삭제하려는 웹페이지가 소스 웹사이트에서 삭제 되었는지 여부를 선택한다.

그림 90 콘텐츠의 삭제 여부 선택



⑥ 캐시 URL의 상태 및 노출된 개인정보 작성

캐시 URL의 상태를 선택하고, 노출된 개인정보를 입력하여 삭제 요청한다.

그림 91 캐시 URL 상태 선택



그림 92 노출된 개인정보 입력



⑦ 삭제 여부 확인

삭제 완료 여부를 확인한다.

그림 93 접수 상태 확인



4) Bing(Bing)

인터넷에 노출된 개인정보가 Bing 검색엔진에 의해 2차 노출된 것을 발견하면, 아래와 같은 절차로 웹 마스터 도구에 방문하여 삭제 조치를 수행한다.

그림 94 Bing 검색엔진 2차 노출 방지 조치 절차



① Bing 검색엔진의 웹 마스터 도움말 센터 페이지 접속

빙의 웹 마스터 도구의 도움말 센터(<https://www.bing.com/webmaster/help>)로 이동한다.

그림 95 웹 마스터 도구에서 도움말 센터로 이동



② Bing의 콘텐츠 삭제 페이지 선택

Remove Broken Links/Outdated Cache 탭의 콘텐츠 삭제 페이지 링크를 선택한다.

그림 96 Bing의 콘텐츠 삭제 페이지 링크 선택



③ Bing 로그인

빙의 콘텐츠 삭제 페이지(<http://www.bing.com/webmasters/tools/contentremoval>)로 이동 후 로그인한다.

그림 97 Bing 로그인



④ 오래된 캐시 페이지 삭제

삭제 페이지에서 캐시 페이지 URL을 작성하여 삭제요청한다.

그림 98 Bing 오래된 캐시 페이지 삭제



개인정보 노출 예방수칙

1. 홈페이지 운영·관리자 개인정보 노출 예방수칙
2. 홈페이지 개발자 개인정보 노출 예방수칙

III

개인정보 노출 예방수칙

1 홈페이지 운영·관리자 개인정보 노출 예방수칙

KEY 1 게시물/댓글 작성 시 개인정보 노출 주의 안내

- ▶ 웹사이트 이용자 또는 운영·관리자가 게시판 이용 시 개인정보 노출 예방에 대한 안내를 받을 수 있도록 해당 페이지에 안내문구 및 팝업창 제공



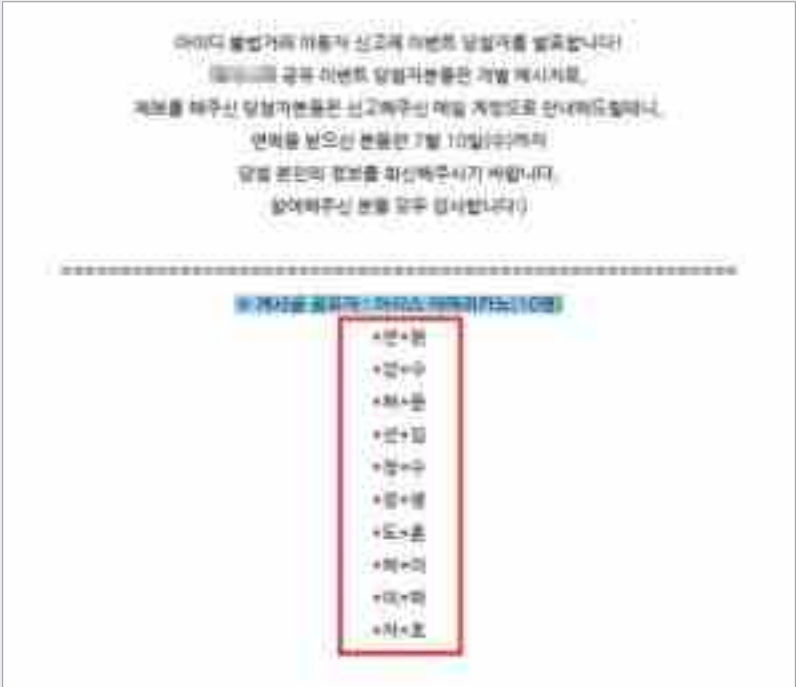
KEY 2 게시물 및 댓글 비공개 설정

- ▶ 게시물에 대한 비공개 여부를 설정할 수 있는 기능 필요

- ▶ 개인정보가 포함되는 민원 페이지나 각종 신청 관련 게시판은 비공개 설정

KEY 3 불가피하게 개인정보가 포함된 게시물 및 게시물·댓글은 비식별 처리

▶ 이벤트 당첨, 합격자 공개 시 개인정보 마스크



KEY 4 파일 업로드 전 개인정보 유무 확인 체크

- ▶ 첨부할 파일에서 불필요한 정보는 삭제 후 게시(업로드)
- ▶ 작성된 첨부 문서에서 개인정보의 포함여부 확인 후 게시(업로드)
 - [엑셀 문서] 숨겨진 시트/행/열에 개인정보가 있는지 확인
 - [엑셀 문서] (메모)에 개인정보가 있는지 확인
 - [엑셀 문서] 배경색과 같은 글자색으로 작성된 개인정보가 있는지 확인
 - [엑셀 문서] OLE 객체(그래프 등)는 더블클릭 후 원본자료에 개인정보가 있는지 확인
 - [엑셀 문서] 외부 파일 참조 기능 활용 여부 및 참조한 외부 파일에 개인정보가 있는지 확인
 - [한글 문서] 한글의 “개인정보 보호 기능”(보기 메뉴)을 이용하여 개인정보 유무 확인
 - [이미지 파일] 이미지 파일에 개인정보 포함 유무 확인
- ▶ 엑셀, 한글 등 편집 가능한 문서의 경우 PDF 파일로 변환하여 게시(업로드)
- ▶ 가능한 경우 개인정보 차단 소프트웨어를 통해 개인정보 사전검색 후 게시

KEY 5 주기적인 개인정보 노출 점검

- ▶ 주기적인 점검 기본사항
 - 검색엔진(구글, 네이버, 다음 등)의 확장기능을 활용하여 개인정보 노출 여부 주기적 점검
 - 가능한 경우 개인정보 탐지 소프트웨어를 활용하여 홈페이지 상 개인정보 존재 유무를 주기적으로 확인
- ▶ 웹사이트 변동(통합, 개선 등)시 점검사항
 - 개인 구분 값으로 개인정보 사용 여부 점검
 - 전송 및 저장 시 개인정보 암호화 여부 점검
 - (개발 시) 시큐어 코딩을 적용하여 개발
 - (개발 후) 시큐어 코딩 준수여부 점검
 - 웹 취약점 점검

2 홈페이지 개발자 개인정보 노출 예방수칙

KEY 1 관리자페이지 접근제어 기능 적용

- ▶ 관리자페이지 접속은 SSL 기술을 이용하여 전송구간 암호화를 적용
- ▶ 관리자페이지는 접속이 필요한 관리자만 접근할 수 있도록 인가된 IP로 제한하는 기능 적용
- ▶ 관리자페이지는 가급적 내부망에서만 연결되도록 구성

● 관리자페이지 접근제한 설정

1. IIS 6.x 이하 웹 서버(윈도우즈 서버)의 경우

- “설정 → 제어판 → 관리도구 → 인터넷 서비스 관리자” 선택
- 해당 관리자페이지 폴더에 마우스 오른쪽 버튼 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. IIS 7.x 이상 웹 서버(윈도우즈 서버)의 경우

- “설정 → 제어판 → 관리도구 → 인터넷 서비스 관리자” 선택
- 해당 관리자페이지 폴더 → IP 주소 및 도메인 이름 제한 → 기능 설정 편집
- ‘지정되지 않은 클라이언트에 대한 액세스’를 거부로 설정(전체 접속 차단)



- 접속 허용할 IP주소 입력



3. Tomcat 서버의 경우

- 환경설정파일 server.xml의 <Host>...</Host>안에 아래의 내용을 추가 후 재시작

Tomcat 서버설정 예

```
<Host>
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="허용할 IP"/>
```

또는

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
deny="거부할 IP"/>
</Context>
</Host>
```

KEY 2 게시물을 비공개와 공개로 구분할 수 있도록 기능 적용

- ▶ 게시물에 개인정보 포함 시 비공개로 설정할 수 있는 기능 적용
- ▶ 비공개 글은 작성자만 열람할 수 있도록 적용



KEY 3 접속경로(URL)에 개인정보 삭제

- ▶ 회원정보 페이지 개발 시 접속경로(URL)에 생년월일, 주민등록번호 등 사용 금지
ex) <http://www.test.or.kr/board.php?search=info&list=19501111>
- ▶ 소스코드 내에 회원 식별자로 주민등록번호 등 사용 금지



KEY 4 홈페이지 설계 시 POST 방식 이용

- ▶ 웹 브라우저 주소 표시줄에 개인정보가 노출되지 않도록 GET 방식 보다는 POST 방식을 사용
 - URL내 개인정보 등이 노출되지 않도록 POST 방식을 이용
 - ex) <http://www.test.or.kr/board.php?search=info&list=19501111>

KEY 5 소스코드 등을 통한 개인정보 및 서버정보 노출 사전점검

- ▶ 소스코드 내 개인정보 및 서버정보 포함여부 점검



- Chrome, Internet Explorer, Safari 등 상용 브라우저 내 소스코드 보기 및 개발자 도구를 이용하여 페이지 소스 내 개인정보, 서버정보 포함여부 점검





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



- 개발단계에서 디버깅 및 테스트를 목적으로 작성한 주석구문에 서버 주요 정보가 포함되어 있을 경우 공격자가 해당 정보를 다른 취약점과 연계해 사용할 수 있으므로 제거

▶ 에러페이지 내 서버정보 포함여부 점검

- 서버별 기본 에러페이지 사용 시, 서버 버전 정보 노출을 비활성화 하더라도 플랫폼 종류의 파악이 가능하므로 자체 에러페이지 사용

1. IIS 웹 서버(윈도우즈 서버)의 경우

- IIS 6.0 웹 서버의 경우

“인터넷 정보 서비스(IIS) → 웹사이트 등록정보 → 사용자 정의 오류”에서 자체
에러페이지 사용 여부 점검



- IIS 7.0 ~ 10.0 웹 서버(윈도우즈 서버)의 경우

“인터넷 정보 서비스(IIS) → 오류페이지 → 기능 설정 편집 → 사용자 지정
오류 페이지”에서 자체 에러페이지 사용 여부 점검



2. Tomcat 서버의 경우

- \$TOMCAT_HOME(톰캣 홈 디렉터리)/conf/web.xml 파일의 Default Welcome File List 항목에 자체 에러페이지 설정 추가
- 에러페이지 설정 추가 후 Tomcat 서버의 ROOT 디렉터리 안에 설정한 이름의 에러페이지를 제작하여 위치

Tomcat 서버설정 예

```
<!-- ===== Default Welcome File List ===== -->
....
    <welcome-file-list>
        <welcome-file>index.html</welcome-file>
        <welcome-file>index.htm</welcome-file>
        <welcome-file>index.jsp</welcome-file>
    </welcome-file-list>

    <error-page>
        <error-code>404</error-code>
        <location>/error-404.html</location>
    </error-page>

</web-app>
```

3. Nginx 서버의 경우

- \$NGINX_HOME(톰캣 홈 디렉터리)/conf/nginx.conf 파일의 error_page 항목에 자체 에러페이지 설정 추가

nginx 서버설정 예

```
server {
    listen 443 ssl;
    server_name www.test.com
    ....
    location / {
        proxy_pass          http://127.0.0.1:7777;
        ....
    }

    error_page 403 404 405 411 497 500 501 502 503 504 505 /error.html;
    location = /error.html {
        root /usr/share/nginx/html;
    }
}
```

KEY 6 주기적인 디렉터리 리스팅 취약점 점검

▶ 주기적인 점검 기본사항

- 검색엔진(구글, 네이버, 다음 등) 확장기능을 이용하여 홈페이지의 관리자페이지가 리스팅되고 있는지 주기적으로 점검
(웹 서버의 url, 도메인 이름, 디렉터리 경로 등을 활용하여 디렉터리 리스팅 여부 점검)

▶ 디렉터리 리스팅 노출 방지 설정

- [Apache] indexes “문자열” 제거
- [Tomcat] Param-value 값을 “False” 로 설정
- [Nginx] Autoindex 값을 “off”로 설정
- [윈도우 인터넷 정보서비스(IIS)] 제어판 → 관리도구 → 인터넷서비스 관리자 → 기본 웹사이트 속성 정보 수정(디렉터리 검색 부분을 비활성화)

※ 자세한 사항은 71페이지 디렉터리 리스팅 보안설정 조치방법 참고

**홈페이지
개인정보
노출방지
안내서**

FAQ

무엇이든 물어보세요

FAQ

무엇이든 물어보세요

Q

개인정보 노출과 유출의 차이점은 무엇인가요?

A

개인정보 노출은 '홈페이지 상 개인정보를 누구든지 알아볼 수 있어 개인정보 유출로 이어질 수 있는 상태'로 단순히 게시판에 개인정보가 게시되어 있다면 노출에 해당하지만 이미 다른 사람이 접근하거나 다운로드하였다면 이는 유출에 해당합니다.

개인정보가 노출되었다면 이를 신속하게 삭제하거나 비공개 처리해야 하며, 제3자가 개인정보에 접근하여 유출로 판단된다면 정보주체에게 유출통지하고 관계 기관에 신고(개인정보처리자: 1천명 이상, 정보통신서비스 제공자등: 1명 이상)하는 등의 조치를 취해야 합니다.

※ 자세한 유출 통지 방법 등은 「개인정보 보호법 제34조, 제39조의4」 등 관련 법령 참고

참고

표준 개인정보 보호지침 제25조(개인정보의 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

Q

홈페이지에 노출된 개인정보는 반드시 삭제, 마스킹, 차단 등 조치해야 하나요?

A

개인정보가 노출될 경우, 다른 사람이 접근하거나 다운로드하는 등 유출될 가능성이 커지게 됩니다.

개인정보가 유출될 경우 관계 법령에 의해 처벌 받을 수 있으므로 신속한 삭제, 마스킹, 차단 등 적절한 조치가 필요합니다. 다만, 다른 사람이 게시하거나 공개한 개인정보를 삭제할 때에는 임의 삭제 조치가 타인의 표현의 자유 및 재산권 등을 침해할 우려가 있는지 확인 후 조치하여야 하며, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 개인정보를 공개하도록 한 경우인지 또한 확인하여야 합니다.

참고

개인정보 보호법 제39조의10(노출된 개인정보의 삭제·차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다.

② 제1항에도 불구하고 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우 정보통신서비스 제공자등은 삭제·차단 등 필요한 조치를 취하여야 한다.

Q

공무원이나 공공기관 임직원 정보(이름, 전화번호 등)를 홈페이지를 통해 공개해도 되나요?

이 경우 공개 가능한 개인정보는 어떤 것이 있나요?

A

공무원이나 공공기관 임직원 정보는 정보공개법 제9조제1항에 의거 홈페이지를 통해 공개 가능 합니다.

공무원 및 공공기관 임직원은 원활한 대민서비스 등 국민의 편의를 진작하고 친절한 서비스 제공 등의 업무진행을 위하여 [조직(부서명), 성명, 사무실 전화번호, 직급/직위, 담당업무] 정도를 기관이나 조직의 홈페이지에 공개하는 것이 일반적입니다.

그러나 집주소, 개인 휴대전화번호, 학력 및 경력 등은 업무와 직결되지 않으므로 공개하지 않아야 합니다. 또한, 랜섬웨어나 악성코드를 삽입한 이메일을 발송하는 등 범죄 악용 우려를 고려해 볼 때 업무상 이메일주소는 공개하지 않는 것이 바람직할 것입니다.

참 고

정보공개법 제9조(비공개 대상 정보) ① 공공기관이 보유·관리하는 정보는 공개 대상이 된다. 다만, 각 호의 어느 하나에 해당하는 정보는 공개하지 아니할 수 있다.

6. 해당 정보에 포함되어 있는 성명·주민등록번호 등 개인에 관한 사항으로서 공개될 경우 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보. 다만, 다음 각 목에 열거한 개인에 관한 정보는 제외한다.

가. 법령에서 정하는 바에 따라 열람할 수 있는 정보

나. 공공기관이 공표를 목적으로 작성하거나 취득한 정보로서 사생활의 비밀 또는 자유를 부당하게 침해하지 아니하는 정보

다. 공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익이나 개인의 권리 구제를 위하여 필요하다고 인정되는 정보

라. 직무를 수행한 공무원의 성명·직위

마. 공개하는 것이 공익을 위하여 필요한 경우로서 법령에 따라 국가 또는 지방자치 단체가 업무의 일부를 위탁 또는 위촉한 개인의 성명·직업

Q

홈페이지를 통해 청년구직수당 등 각종 수당 지급대상자를 발표·공개하려고 합니다.

수급자의 개인정보는 어느 범위까지 공개 가능한가요?

A

청년구직수당 등 각종 수당지급 대상자의 경우 개별적으로 연락하는 것이 권장됩니다. 부득이 홈페이지를 통해 공개해야할 경우 지원자 본인만 확인할 수 있도록 개인정보를 마스킹 처리하는 것이 바람직합니다.

Q

홈페이지를 통해 채용 합격자 발표 시 합격자의 개인정보는 어느 범위까지 공개 가능한가요?

A

원칙적으로 합격자 발표는 개별적으로 연락하는 것이 권장됩니다. 그럼에도 불구하고 홈페이지에서 합격자를 공개해야하는 경우 개인정보 보호법 제3조제7항에 의거 지원자 본인만 확인할 수 있도록 응시번호 또는 수험번호만 기재하는 것이 바람직합니다. 다만, 동명이인의 구별 등을 위하여 성명 이외의 다른 정보(생년월일, 아이디, 연락처 등)를 함께 게시하는 경우에는, 성명의 일부 마스킹과 함께 생년월일이나 연락처 등도 일부를 마스킹 하여 식별되지 않도록 해야 합니다.

참고

개인정보 보호법 제3조(개인정보 보호 원칙) ⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

Q

학원을 홍보하기 위해 홈페이지에서 학원생들의 각종 경진대회, 공모전, 콩쿠르 등의 입상 결과 (이름, 사진, 학교, 학년 등)를 공개해도 되나요?

A

학원이 학원생들의 입상결과 공개와 관련하여 사전 동의를 받았을 경우에만 공개할 수 있습니다. 이 때 학원생이 만 14세 미만일 경우 개인정보 보호법 제22조(동의를 받는 방법)제6항에 따라 법정대리인의 동의(학생이 만 14세 미만일 경우)를 받아야 합니다.

만일 입상결과 공개와 관련하여 동의 받지 않고 후에 공개할 경우 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)에 따라 처벌 받을 수 있습니다.

참고

개인정보 보호법 제22조(동의를 받는 방법) ⑥ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항 및 제39조의3제1항 및 제2항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

Q

홈페이지 게시판에 이용자가 자신 또는 타인의 개인정보를 스스로 게재하는 경우에도 홈페이지 운영·관리자가 관리해야 하나요?

A

개인정보 보호법 제3조(개인정보 보호 원칙)제4항 및 제39조의10(노출된 개인정보의 삭제·차단) 등에 의거 홈페이지 운영·관리자는 이용자 개인정보 게재 행위까지도 관리해야 합니다. 홈페이지 운영·관리자는 홈페이지 내 주의 문구를 삽입하여 이용자가 홈페이지에 개인정보를 게재하지 않도록 안내해야 합니다.

※ 자세한 사항은 53페이지 '개인정보 노출에 대한 경고문구 삽입 예시' 참고

참고

제3조(개인정보 보호 원칙) ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

개인정보 보호법 제39조의10(노출된 개인정보의 삭제·차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다.

② 제1항에도 불구하고 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우 정보통신서비스 제공자등은 삭제·차단 등 필요한 조치를 취하여야 한다.

Q

동호(창)회 회원들의 친목 도모를 목적으로 홈페이지를 통해 회원 연락처를 게시·공유해도 되나요?

A

동호(창)회 회원들의 친목 도모를 위해 회원 간에 연락처를 공유하는 경우라면 개인정보 보호법 제58조제3항에 의거 홈페이지에 권한없는 제3자가 접근하지 못하도록 비공개 설정하여 공유해도 됩니다. 단, 관련법령은 제15조(개인정보의 수집·이용), 제30조(개인정보처리방침 수립·공개), 제31조(개인정보 보호책임자 지정)에 한해서만 제외되고 나머지 법조항은 모두 적용됩니다. 따라서 목적 외 이용, 제3자 제공, 안전성 확보조치 수립 등의 의무는 여전히 부과되므로 회원에 한해서만 열람 가능하도록 주의하고, 친목 도모 외의 목적으로 이용하거나, 회원이 아닌 제3자에게 정보를 제공해서는 안 됩니다.

참 고

개인정보 보호법 제58조(적용의 일부 제외) ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

Q

홈페이지 게시판에 일부 회원의 개인정보가 노출되어 있는 것을 확인하고 즉시 삭제 조치했는데도, 구글 등 검색사이트에서 해당 게시물이 계속 검색됩니다. 어떻게 해야 하나요?

A

노출된 개인정보를 해당 웹사이트에서 삭제하였더라도 구글 등 검색 사이트에 기 노출된 정보가 저장되어 검색 시 2차 노출될 수 있습니다. 따라서 75페이지(나. 검색엔진을 통한 2차 노출 방지 방안)를 참고하여 검색사이트에 저장된 페이지를 삭제해야 합니다.

Q

소규모 비영리 단체 홈페이지를 운영하고 있는데, 웹 취약점 점검을 반드시 받아야 하나요?

A

개인정보의 안전성 확보조치 기준 제6조제8항에 따르면 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인은 웹 취약점 점검 대상이 아닙니다. 반면, 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인은 웹 취약점 점검을 연 1회 이상 수행해야 합니다.

KISA 인터넷보호나라&KrCERT(www.krcert.or.kr)에서 웹 취약점 점검을 무료로 서비스하고 있습니다. 해당 서비스는 '중소기업기본법 제2조'에 해당하는 중소기업까지 제공되므로, 소규모 비영리 단체 또한 이용할 수 있습니다.

참고

개인정보의 안전성 확보조치 기준 제6조(접근통제) ④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보안 조치를 하여야 한다. ⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

그림 99 KISA 인터넷 보호나라 웹 취약점 점검 신청 페이지

Q

홈페이지에서 검색엔진 등의 크롤링을 통해 개인정보가 노출되지 않도록 개인정보의 안전성 확보조치를 이행해야 하는 것과는 별개로, 다른 홈페이지에 공개되어 있는 개인정보가 포함된 데이터를 크롤링을 통해 수집하여 활용할 때 유의해야 할 기준이나 판례가 있나요?

A

자신의 홈페이지에 게재된 정보가 검색엔진 등 다른 사업자의 크롤링을 통해 수집되는 경우에는 개인정보가 노출되지 않도록 안전성 확보 조치를 이행하여야 합니다.

이와 별개로, 다른 웹사이트에 게재된 정보를 크롤링을 통해 수집하여 활용하고자 하는 경우에는 다음의 사항을 유의하여 운영해야 합니다. 공개된 정보(데이터)에 대한 크롤링 자체를 제한하고 있는 규정은 없으나, 크롤링하여 수집한 정보에 개인정보가 포함되어 있고 정보주체가 동의한 것인지 여부가 모호한 경우에는 개인정보 침해 이슈가 발생할 가능성이 있습니다. 크롤링을 통한 개인정보 처리와 관련된 직접적인 판례는 없으나, 대법원은 공개된 개인정보도 개인정보에 해당하고 이미 공개된 개인정보를 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 처리할 때는 동의는 불필요하다고 판시한 사례가 있습니다. (대법원 2016.8.17. 선고 2014다235080 판결)

따라서, 크롤링에 의해 수집한 공개된 개인정보가 정보주체의 동의가 있었다고 객관적으로 인정되기 어려운 경우에는 크롤링 과정에서 개인정보가 수집·저장되지 않도록 조치할 필요가 있습니다.

※ (사례) 접근통제가 되어 있지 않은 웹사이트의 회원정보를 크롤링을 통해 수집한 경우, 게시판 등에 잘못 올린 개인정보를 크롤링으로 수집한 경우 등

참고

크롤링을 통해 웹사이트 운영자의 의사에 반하여 접근권한없이 접속한 경우에는 정보통신망법 위반으로 형사처벌을 받을 수 있다는 점을 유의해야 합니다. 예를 들어, 경쟁관계에 있는 A사가 B사의 웹사이트에 접근권한없이 무단으로 접속한 후 고의적으로 크롤링하여 B사의 정보를 수집·이용할 경우에는 '타인의 정보통신망에 대한 무단침입'에 해당할 수 있습니다.

※ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조 제1항: 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니된다.

정보통신망 무단침입을 통해 개인정보가 유출된 경우에는 유출된 웹사이트도 개인정보의 안전성 확보조치 미이행 시에는 개인정보 보호법*에 따라 형벌, 과징금, 과태료 부과 대상에 해당될 수 있습니다.

* 개인정보보호법 제39조의15(과징금), 제73조(벌칙), 제75조(과태료)

홈페이지
개인정보
노출방지
안내서

부록

- 부록 1 주요 용어 이해하기
- 부록 2 개인정보 노출 점검, 스스로 해보기
- 부록 3 개인정보 유출 시 필수 조치사항
- 부록 4 주요 개인정보 8종 정규표현식
- 부록 5 참고자료

부록 1

주요 용어 이해하기

이 안내서에서 사용하는 용어의 뜻은 다음과 같다.

용어	용어 정의
개인정보 마스킹	개인정보 보호를 위해 주민등록번호, 의료보험번호, 여권번호, 운전면허번호 등 개인정보의 일부가 식별되지 않도록 조치하는 것이다.
개인정보 차단 소프트웨어	웹사이트에 자료를 올리거나, 게시판에 글 작성 시 콘텐츠에 개인정보 존재 유무를 확인해주는 솔루션이다.
개인정보 탐지 소프트웨어	웹사이트 내에 존재하는 개인정보를 검색하여 개인정보의 위치를 확인해주는 솔루션이다.
개인정보	“개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다. 다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다) (개인정보 보호법 제2조제1호)
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 말한다. (개인정보 보호법 제2조제2호)
개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. (개인정보 보호법 제2조제5호)
개인정보취급자	개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자를 뜻한다. (개인정보 보호법 제28조제1항)
검색엔진 (Search Engine)	검색엔진이란 인터넷 상에서 자료를 쉽게 찾을 수 있도록 검색사이트에 구축된 시스템이다. 검색엔진은 정보수집·정보가공·정보제공의 세 가지 기능으로 구성 되는데 정보수집은 크롤러, 정보가공은 인덱서, 정보제공은 사용자 인터페이스가 담당한다. 크롤러가 인터넷을 검색하여 수집한 정보들을 인덱서를 이용하여 데이터베이스화 하고, 사용자가 검색어를 입력하면 사용자 인터페이스가 관련된 정보의 위치를 알려 준다.

용어	용어 정의
공공기관	개인정보 보호법 제2조에 따르면 공공기관은 다음과 같다. 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관 (개인정보 보호법 제2조제6호)
동적 홈페이지	html 태그 안에 자바스크립트, JSP등의 홈페이지 언어를 사용하여 홈페이지 사용자의 요청에 따라 변화하여 다양한 화면을 보여주는 유동적인 홈페이지를 말한다.
디렉터리 리스팅 취약점 (Directory Listing Vulnerability)	WEB이나 FTP 서비스의 취약한 설정으로 인해 서버의 디렉터리, 파일이 열람 및 다운로드가 가능하게 되는 취약점이다. 인터넷 사용자가 모든 디렉터리 및 파일 목록을 볼 수 있어 비공개 자료가 유출될 수 있다.
디렉터리 (Directory)	디지털 자료 저장장치인 하드디스크에 저장된 파일들을 담고 있는 영역을 말하며, 디렉터리에는 그 속에 저장된 각각의 파일에 대한 이름과 크기, 위치 등이 기록되어 있다.
디버깅 (Debugging)	컴퓨터 프로그램의 오류를 찾아내고 수정하는 작업을 말한다.
보이스피싱 (Voice Phishing)	전화를 통해 불법적으로 개인정보(주민등록번호, 신용카드번호, 은행계좌번호 등)를 빼내 범죄에 사용하는 신종 전화 사기 수법이다. 음성(voice), 개인 정보(personal information) 및 낚시(fishing)를 합성한 신조어이다. 기존의 피싱은 이메일을 통해 중요 정보를 입력하게 하는 소극적인 방법인 데 반해, 보이스피싱은 범행 대상자에게 전화를 걸어 송금을 요구하거나 개인정보를 수집하는 적극적인 방법이다.
소스코드 (Source Code)	컴퓨터 프로그램을(사람이 읽을 수 있는) 프로그래밍 언어로 기술한 글을 말한다.
스팸 (Spam)	수신자의 의사와 관계없이 인터넷상의 다수 수신인에게 전자 우편(e-mail), 문자메시지 등을 이용하여 무더기로 발송한 광고나 선전물을 의미한다.
시큐어 코딩	개발하는 소프트웨어가 복잡해짐으로 인해 보안상 취약점이 발생할 수 있는 부분을 보완하여 프로그래밍하는 것이다. 시큐어 코딩에는 안전한 소프트웨어를 개발하기 위해 지켜야 할 코딩 규칙과 소스 코드 취약 목록이 포함된다.
엑셀 (Excel)	미국 마이크로소프트(MS)사에서 개발한 PC용 수치관리 프로그램을 의미한다. 많은 스프레드시트를 연결, 통합하여 다양한 도형과 차트 등 설명 자료를 작성하는 기능을 제공한다.
웹 서버 (Web Server)	웹페이지가 들어 있는 파일을 사용자들에게 제공하는 프로그램이다. 웹사이트를 통해 서비스하려면 웹 서버 프로그램을 설치해야 한다. 포편적인 웹 서버로는 IIS와 아파치 등이 있다.
전용선	보안 등을 이유로 연결되는 노드 간에 독점 사용하는 회선을 말한다.
정규표현식	특정한 규칙을 가진 문자열의 집합을 표현하는 데 사용하는 형식 언어다. 정규표현식은 많은 텍스트 편집기와 프로그래밍 언어에서 문자열의 검색과 치환을 위해 사용되고 있다.
정보주체	처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다. (개인정보 보호법 제2조제3호)

용어	용어 정의
정적 홈페이지	일반 html태그만으로 작성되어 변화 없이 일정한 화면을 보여주는 페이지를 말한다.
캐시 (Cache)	데이터 접근을 빠르게 할 수 있도록 데이터를 일시 저장해 두는 장소를 말한다.
크롤러 (수집기)	검색엔진의 정보수집 부분을 담당하는 소프트웨어로 방대한 웹페이지를 주기적으로 방문하여 각종 정보를 자동으로 수집한다. 스파이더, 로봇, 봇, 웹수집기, 로봇 에이전트 등 다양한 이름으로 불리기도 한다.
팝업창	특정 웹사이트가 어떠한 내용을 표시하기 위해 추가로 생성하는 새 창을 말한다.
포워드 (Forward)	클라이언트가 접속한 서버에서 다른 서버로 페이지 변경이 발생하는 경우를 말한다.
포털사이트 (Portal Site)	인터넷의 출발점과 관문이 되는 사이트를 말하는데, 초기에는 인터넷을 항해하기 위한 출발점으로서의 역할만을 수행하였다. 그러나 현재는 특정 주제를 가지고 한 영역에서 전문정보를 제공하는 사이트나 필요한 모든 서비스를 한 곳에서 제공하는 사이트를 의미한다.
하드코딩	변수의 값을 고정하여 코딩하는 것을 말한다.
홈페이지 개발자	홈페이지를 설계·구축·보수하는 자를 말한다. 홈페이지 개발 과정에서 개인정보를 처리하는 경우 개인정보 보호법에 따른 개인정보처리자 또는 개인정보취급자에 해당한다.
홈페이지 운영·관리자	홈페이지를 안전하고 체계적으로 운영 또는 관리하고 이용자에게 각종 서비스를 제공하는 자를 말한다. 홈페이지에서 개인정보를 처리하는 경우 개인정보 보호법에 따른 개인정보처리자 또는 개인정보취급자에 해당한다.
휴면 웹사이트	휴면 웹사이트는 장기간 동안 접속자가 없거나 관리가 이루어지지 않고 방치된 웹사이트를 말한다.
DB 서버 (Database Server)	데이터베이스가 구동되는 서버로 데이터베이스에 대한 요청(검색과 보관)을 처리하여 그 결과를 보내는 것이다.
OLE (Object Linking and Embedding)	응용 프로그램 간 서로 호환이 되어 다른 응용 프로그램에서 작성한 그림이나 표, 차트, 비디오 등과 같은 데이터의 정보를 연결시켜 주는 기능을 뜻한다.
SSL (Secure Sockets Layer)	인터넷 프로토콜(Internet protocol)이 보안면에서 기밀성을 유지하지 못한다는 문제를 극복하기 위해 개발되었다. 인터넷 상거래 시 요구되는 개인정보와 신용카드정보 등의 보안 유지에 가장 많이 사용되고 있다.
URL (Uniform Resource Locator)	흔히 웹사이트 주소로 알려져 있지만, 이는 웹 사이트 주소뿐만 아니라 컴퓨터 네트워크 상의 모든 자원을 나타낼 수 있다. URL은 주 컴퓨터의 이름과 주소, 파일이 있는 디렉터리 위치, 파일 이름으로 구성된다.
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 전용선의 고비용 부담을 해소하기 위해 사용한다.
WAS 서버 (Web Application Server)	브라우저 클라이언트로부터 HTTP요청을 받아들이고 HTML 등의 웹페이지 문서에 반응하는 서버를 말한다.

부록 2

개인정보 노출 점검, 스스로 해보기

홈페이지를 운영하는 기관·기업은 자사 사이트에서 개인정보가 노출되고 있는지 검색엔진을 통해 모니터링할 수 있다. 홈페이지 운영자 또는 관리자는 자신이 관리하는 사이트에서 검색엔진에 의한 개인정보 노출이 있는지 주기적으로 점검하고 검색엔진에 개인정보가 노출되었다면 즉시 조치를 취해야 한다. 네이버, 구글 등 검색엔진의 기본검색이나 고급검색 기능을 활용하여 점검할 수 있다.

참고

주요 노출 키워드(예시)

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

1단계 (구글(google.co.kr)에 접속)

그림 100 구글 검색 화면



2단계 (기본검색/고급검색을 사용하여 개인정보 자가 점검 수행)

1) 기본검색

구글 기본검색은 검색어를 입력하여 특정 검색어를 포함하거나, 특정 검색어를 제외하여 검색하는 등 기본적인 검색 기능을 제공한다.

연산자	설명	형식
" "	정확한 문구를 포함한 결과 검색	"검색어"
~	검색어와 비슷한 결과 검색	~검색어
and, 공백	둘 다 포함한 결과 검색	검색어A and 검색어B
OR(대문자),	둘 중에 하나 포함한 결과 검색	검색어A 검색어B
-(마이너스)	원하지 않는 단어를 제외한 결과 검색	-검색어

2) 고급검색

고급검색은 검색 범위를 특정 사이트로 제한하거나, 특정 파일만 검색하는 등 특정 명령어를 이용하여 원하는 결과 값을 쉽게 얻을 수 있는 기능이다.

명령어	설명	형식
define	특정 단어의 정의 검색	define:검색어
site	검색 범위를 특정 도메인으로 제한 검색	site:kisa.or.kr 검색어
intitle	페이지의 제목에서 문자열 검색	intitle:검색어
inurl	문자열을 페이지의 URL에서 검색	inurl:검색어
filetype	특정한 확장자를 가진 파일 검색	filetype:'파일형식'
numrange	- 앞뒤로 지정된 숫자 범위 안에 있는 결과 검색	numrange #-# 검색어

기본검색 또는 고급검색을 이용하여 개인정보 유·노출 여부를 점검한다.

그림 101 구글 고급검색 예시



부록 3

개인정보 유출 시 필수 조치사항

온·오프라인을 통해 개인정보를 수집·이용하는 기관이나 기업은 해킹 등으로 개인정보 유출이 발생한 경우 개인정보 보호 관련 법령에 따라 해당 정보주체(이용자)에게 지체 없이 통지하여야 한다. 또한, 개인정보 유출로 인한 피해를 최소화하기 위해 필요한 긴급 조치를 이행하고, 그 조치 결과를 개인정보보호위원회 또는 한국인터넷진흥원에 지체 없이 신고하여야 한다.

정부·공공기관 및 비영리 협·단체 등의 경우, 개인정보가 유출되었음을 알게 된 후 5일 이내 정보주체에게 통지해야 하며, 1천명 이상 정보주체의 개인정보 유출 시에는 개인정보보호위원회 또는 한국인터넷진흥원(www.privacy.go.kr)에 신고해야 한다.

한편, 정보통신서비스 제공자등은 1명 이상 이용자의 개인정보 유출이 발생한 경우, 유출되었음을 알게 된 후 24시간 이내 해당 이용자에게 개인정보 유출 통지를 해야 하며, 개인정보보호위원회 또는 한국인터넷진흥원(www.privacy.go.kr)에 신고해야 한다.

그림 102 개인정보 유출 시 필수 조치요령

개인정보 유출 시 필수 조치요령

Korea Internet & Security Agency

01

신속 통지

유출된 정보주체 개개인에게 지체 없이 통지

| 시 한 | 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)

| 통지항목 |

- 1 유출된 개인정보의 항목
- 2 유출 시점 및 그 경위
- 3 피해 최소화를 위한 정보주체의 조치방법
- 4 기관의 대응조치 및 피해구제 절차
- 5 피해 신고 접수 담당부서 및 연락처

※ 정보통신서비스 제공자등은 유출되었음을 알게된 후 (24시간 이내)

02

긴급 조치

피해 최소화 위한 대책 마련 및 필요한 조치 실시

| 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급 조치 이행

| 긴급 조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청

03

대량 유출

1천 명 이상 유출된 경우 유출 통지 결과를 신고하고 홈페이지에 공지

| 1천 명 이상 개인정보가 유출된 경우 유출 통지 및 조치결과를 지체 없이 개인정보보호위원회 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고

※ 정보통신서비스 제공자등은 1명 이상 이용자의 개인정보 유출이 발생한 경우 유출 신고

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

I 개요

II 개인정보 노출원인 및 조치방안

III 개인정보 노출 예방수칙

FAQ 무엇이든 물어보세요

부록

참 고

「개인정보 보호법」 상의 개인정보 유출 통지·신고 근거 법령

〈 개인정보 보호법 〉

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
 2. 유출된 시점과 그 경위
 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해 구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
- ③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.
- ④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

〈 개인정보 보호법 시행령 〉

제40조(개인정보 유출 통지의 방법 및 절차) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면등의 방법으로 지체 없이 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.

② 제1항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제34조제1항제1호 및 제2호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

③ 제1항과 제2항에도 불구하고 법 제34조제3항 및 이 영 제39조제1항에 따라 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 7일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 7일 이상 게시하여야 한다.

참고

〈 개인정보 보호법 〉

제39조의4(개인정보 유출등의 통지·신고에 대한 특례) ① 제34조제1항 및 제3항에도 불구하고 정보통신서비스 제공자와 그로부터 제17조제1항에 따라 이용자의 개인정보를 제공받은 자(이하 “정보통신서비스 제공자등”이라 한다)는 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 사항을 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 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.

1. 유출등이 된 개인정보 항목
 2. 유출등이 발생한 시점
 3. 이용자가 취할 수 있는 조치
 4. 정보통신서비스 제공자등의 대응 조치
 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
- ② 제1항의 신고를 받은 대통령령으로 정하는 전문기관은 지체 없이 그 사실을 보호위원회에 알려야 한다.
- ③ 정보통신서비스 제공자등은 제1항에 따른 정당한 사유를 보호위원회에 소명하여야 한다.
- ④ 제1항에 따른 통지 및 신고의 방법·절차 등에 필요한 사항은 대통령령으로 정한다.

〈 개인정보 보호법 시행령 〉

제48조의4(개인정보 유출 등의 통지·신고에 관한 특례) ① 법 제39조의4제1항 각 호 외의 부분 본문 및 제2항에서 “대통령령으로 정하는 전문기관”이란 한국인터넷진흥원을 말한다.

- ② 정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.
- ③ 정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고해야 한다.
- ④ 정보통신서비스 제공자등은 법 제39조의4제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제39조의4제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제2항의 통지를 갈음할 수 있다.
- ⑤ 천재지변이나 그 밖의 부득이한 사유로 제4항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하는 것으로 제4항에 따른 홈페이지 게시를 갈음할 수 있다.
- ⑥ 정보통신서비스 제공자등은 법 제39조의4제1항 각 호 외의 부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면으로 보호위원회에 소명해야 한다.

개인정보보호 포털(www.privacy.go.kr)을 통한 개인정보 유출 신고 절차는 다음과 같다.

① 개인정보보호 포털(www.privacy.go.kr) 접속



② 민원마당 - '개인정보 유출·침해신고' 클릭



부록 4

주요 개인정보 8종 정규표현식

인터넷 상 개인정보 노출 모니터링을 위한 주요 개인정보 8종의 정규표현식은 다음과 같다.

● 주요 개인정보 8종 정규표현식

▶ 주민등록번호

(?<=[^0-9a-zA-Z])([0-9][0-9][01][0-9][0-3][0-9][\s-:~.])?(?([1-4]\d{6})?(=[^0-9a-zA-Z])

▶ 여권번호

(?<=[^0-9a-zA-Z])([M|S|R|O|D|m|s|r|o|d][0-9]{8})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])([a-zA-Z]{2}[0-9]{7})?(=[^0-9a-zA-Z])

▶ 운전면허번호

(?<=[^0-9a-zA-Z])(\d{2}[\s-:~.])\d{6}[\s-:~.])\d{2})?(=[^0-9a-zA-Z])

▶ 휴대전화번호

(?<=[^0-9a-zA-Z])(01[0116789]|\s-:~.])?\d{3,4}[\s-:~.])?\d{4})?(=[^0-9a-zA-Z])

▶ 신용카드번호

(?<=[^0-9a-zA-Z])(\d{4}[\s-:~.])\d{4}[\s-:~.])\d{4}[\s-:~.])\d{4})?(=[^0-9a-zA-Z])

▶ 건강보험번호

(?<=[^0-9a-zA-Z])([1-9]\d{10})?(=[^0-9a-zA-Z])

▶ 계좌번호

(?<=[^0-9a-zA-Z])(\d{3}[\s-:~.])\d{3}[\s-:~.])\d{6})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])(\d{4}[\s-:~.])\d{3}[\s-:~.])\d{6})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])(\d{6}[\s-:~.])\d{2}[\s-:~.])\d{6})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])(\d{6}[\s-:~.])\d{2}[\s-:~.])\d{6})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])(\d{3}[\s-:~.])\d{2}[\s-:~.])\d{5}[\s-:~.])\d{1})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])(\d{3}[\s-:~.])\d{6}[\s-:~.])\d{5})?(=[^0-9a-zA-Z])

(?<=[^0-9a-zA-Z])(\d{3}[\s-:~.])\d{6}[\s-:~.])\d{2}[\s-:~.])\d{3})?(=[^0-9a-zA-Z])

▶ 외국인등록번호

(?<=[^0-9a-zA-Z])([0-9][0-9][01][0-9][0-3][0-9][\s-:~.])?(?([5-8]\d{6})?(=[^0-9a-zA-Z])

부록 5

참고자료

보다 안전한 홈페이지 구축·운영을 위해 홈페이지 설계·개발 단계부터 운영에 이르기까지 각 단계별로 도움을 받을 수 있는 유용한 공개 참고자료이다.

NO	자료명	다운로드 위치
1	개인정보의 안전성 확보조치 기준 해설서(2019.06.)	KISA → 자료실 → 관련법령·기술안내서 → 기술안내서가이드
2	개인정보의 암호화 조치 안내서(2017.01.)	
3	소프트웨어 개발보안 가이드(2019.11.)	
4	소프트웨어 보안약점 진단가이드(2019.06.)	



개인정보보호위원회



한국인터넷진흥원