홈페이지 개인정보
유·노출 위반사례 및 후속조치

KISA 한국인터넷진흥원

KISA 한국인터넷진흥원

목차

CONTENTS

KISA 한국인터넷진흥원

Ⅰ. 개인정보 유·노출 위반사례

1. 개인정보 유·노출의 개념
2. 개인정보 유·노출로 인한 피해
3. 개인정보 유·노출 사례

KISA 한국인터넷진흥원

1. 개인정보 유·노출의 개념

1 개인정보 유출이란?

2 개인정보 노출이란?

“개인정보”『유출』이란?

정보주체의 “개인정보”에 대하여 개인정보처리자가 통제를 상실하거나
또는 권한 없는 자의 접근을 허용한 경우 (고의+부주의)

노출

- 게시판 상담요청 및 처리 시, 개인정보가 포함된 내용을 그대로 답변 등으로 게시할 경우
- 검색엔진 등을 통한 사이트 내에 개인정보가 수집/저장 되어 일반인이 노출된 개인정보에 접근하게 하는 경우

유출

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

홈페이지를 통한 “개인정보”『노출』이란?

“개인정보 노출” 은 유출의 한 부분

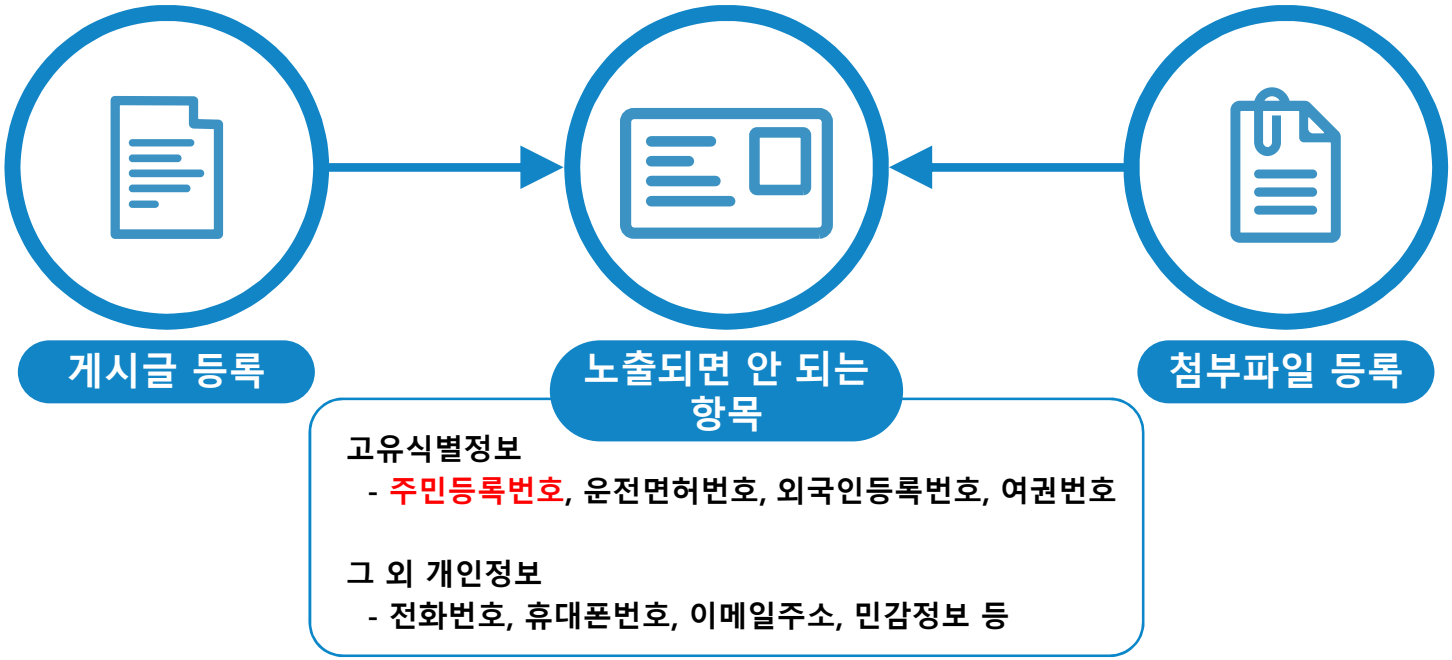
홈페이지 이용자가 해킹 등 특별한 방법을 사용하지 않고, 인터넷을 이용하면서
타인의 개인정보를 취득할 수 있도록 인터넷 상에서 관련 『정보가 방치』된 상태
주로 홈페이지 관리자 및 이용자의 부주의로 발생

➢ 노출과 유출의 차이점

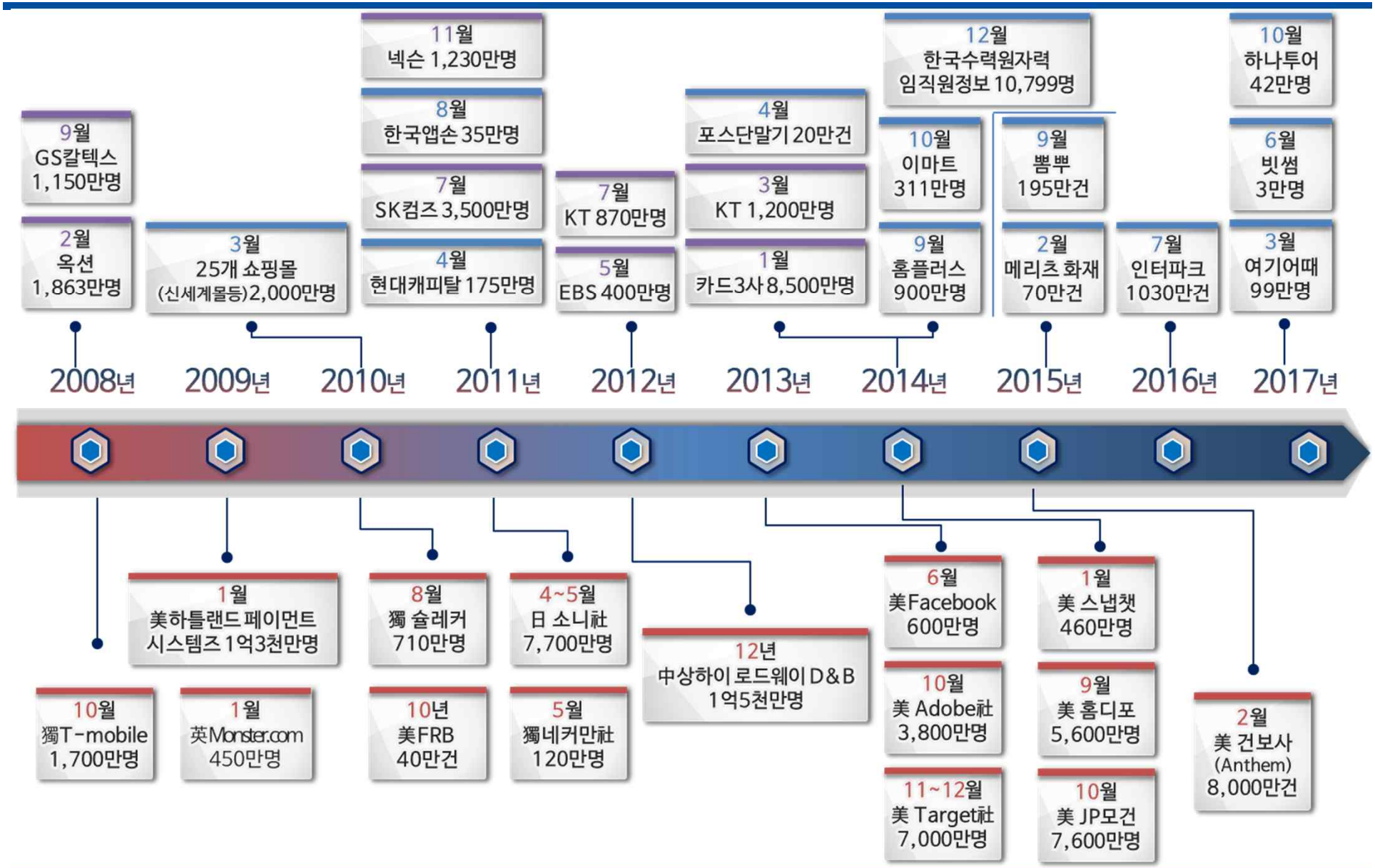
구 분	유 출	노 출
개 념	통제를 상실하거나 권한이 없는 자의 접근을 허용	정보통신망 등을 통하여 공중에 노출
관련법령	개인정보보호법	법적 정의 없음(정통망법)
법적책임	형사처벌대상 (고의, 과실)	형사처벌대상 아님 (부주의)
주 체	내부자, 외부자,(내부+외부자)	내부자

유출과 노출

- 노출 단계에서 신속한 대응 조치 필요
- 노출 -> 유출 -> 개인정보 침해사고
- 홈페이지상에 노출이 빈번히 발생하는 경로 및 노출되면 안되는 항목



국내외 개인정보 유출 현황



KISA 한국인터넷진흥원

2. 개인정보 유·노출로 인한 피해

1. 개인 측면의 피해
2. 기업 측면의 피해
3. 국가 측면의 피해

개인정보 유·노출로 인한 피해

개인정보 침해에 따른 개인/기업/국가의 피해

개인

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

기업

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

국가

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

KISA 한국인터넷진흥원

3. 개인정보 유·노출 예시

1. 개인정보 유출 사례
2. 개인정보 해킹 사례
3. 개인정보 매매 사례
4. 개인정보 오·남용 사례
5. 허술한 관리/방치 사례
6. 홈페이지 노출 사례
7. 기 타

개인정보 유출 신고현황

- 개보법 시행('11.9.30.) 이후(망법포함) '18년까지 개인정보 유출 신고는 총 502건

- '15년 이후 신고 건이 증가 추세, '18년은 전년 대비 약 4배 증가

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

< 년도 별 개인정보 유출 신고 현황 >

관련법	신고기준	신고접수 현황							
		'11년	'12년	'13년	'14년	'15년	'16년	'17년	'18년
개인정보보호법	1천건* 이상/5일 내	1	12	6	40	8	-	14	28
정보통신망법	1건 이상/24시간 내	-	19	7	100	17	40	50	205
합 계		1	31	13	140	25	40	64	233

* '14년은 카드3사 개인정보 유출사고 후 개인정보 유출에 대한 인식 변화로 신고건수가 증가

개인정보 유출 사고 원인

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

  * 유출된 개인정보를 대가로 비트코인을 요구하거나, 개인정보DB를 불법적으로 거래

- 최근 4년간 개인정보 유출(362건)의 80.5%가 해킹 등 외부 공격이 원인

< 개인정보 유출 사고 주요 원인 ('15~'18년) >

외부공격[1]	시스템 오류[2]	내부직원 유출[3]	관리자 부주의[4]	기타[5]
80.5%	6.9%	1.8%	9.0%	1.8
291건	25건	7건	33건	7건

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

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

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

4) 약국 처방전이나 개인정보가 담긴 서류를 미파기 및 방치 등

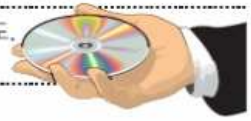
5) 확인불가 등 원인 미상

1. 개인정보 유출 사례(1/2)

- G 정유사 회원정보 관리를 담당하는 자회사 직원이 개인정보 판매 목적으로 고객정보 1,125만건 유출 (2008.9)

GS칼텍스 고객정보 유출 일지

6월 말	용의자 정모(28) 씨, 고객 정보 및 네트워크 관리 업무 배정
7월 10일	정 씨, 고교 동창 왕모(28) 씨와 범행 공모
7월 13일	정 씨, 고객 정보 빼돌려 샘플 CD 제작. 왕 씨의 후배 김모(24) 씨, 범행 합류
8월 27일	정 씨, 동료 직원인 배모(30·여) 씨에게 고객 정보를 엑셀 파일로 정리 부탁
8월 29일	정 씨, 정리된 파일을 DVD로 제작. 왕 씨, 이 DVD를 "언론에 제보해달라"며 김 씨에게 전달
9월 2일	김 씨, 모 언론사 기자 등에게 제보, DVD 5장 복사해 전달
9월 5일	DVD를 전달받은 기자, 고객 정보 유출 사실 보도. 경찰, GS칼텍스의 의뢰로 수사 착수
9월 6일	경찰, 정 씨 일당 검거



1. 개인정보 유출 사례(2/2)

- ○○시 공무원 2명이 시립묘지 연고자 6,449명의 개인정보를 장묘 업체 관계자에 유출

- 교육청 장학사가 교육의원에 출마한 후배를 위해 관내 교직원 3,000명의 이름, 전화번호 등 유출

2. 개인정보 해킹사례

외부자 해킹 유출 사례 _ 과징금 과태료 처분 사례

알툴즈 계정에 등록된 **16만6179명의 개인정보가 중국 해커에게 유출**

방송통신위원회

이스트소프트가 정보통신망법 '**개인정보의 기술·관리적 보호조치 기준**'을 **위반**했다고 판단

과징금 1억2000만원, 과태료 1000만원 등을 처분

3. 개인정보 매매 사례

주민센터 직원이 심부름센터 등에 건당 만원씩 받고 개인정보 판매

C택배회사 영업소장이 자사와 거래하던 홈쇼핑 업체의 고객정보 2백만건을 빼돌려 텔레마케팅 업체에 판매

4. 개인정보 오·남용 사례

- **차량등록시스템에 있는 차량번호, 주민번호, 이름 등 150명의 정보를 다른 공무원으로부터 건네받아 개인적 목적으로 사용**

5. 허술한 관리/방치 사례

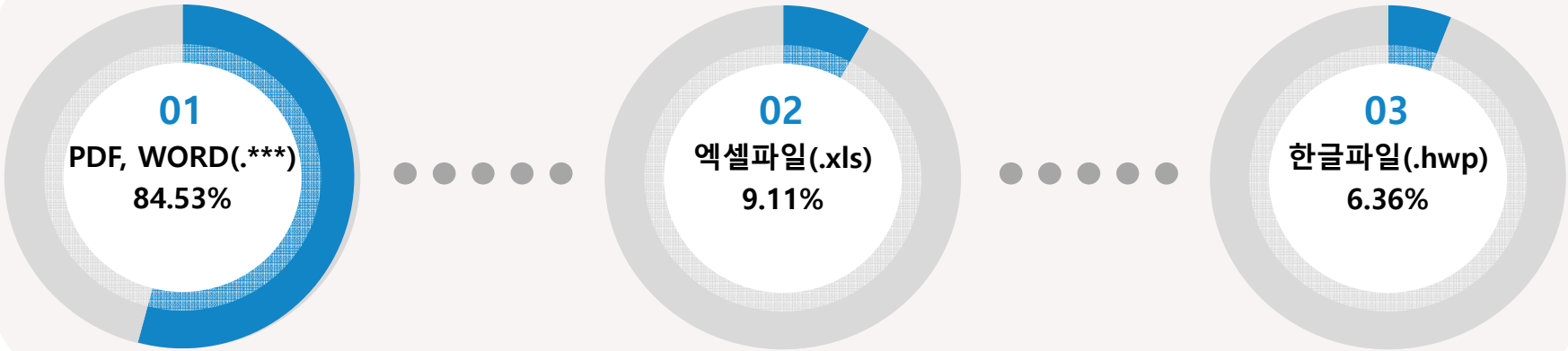
모 공단 직원이 고객정보 10만 건이 기록된 서류 미 파기 및 차량 방치

C 은행 직원의 부주의로 고객의 개인정보가 포함된 리스트를 상품 안내 이메일에 첨부하여 발송

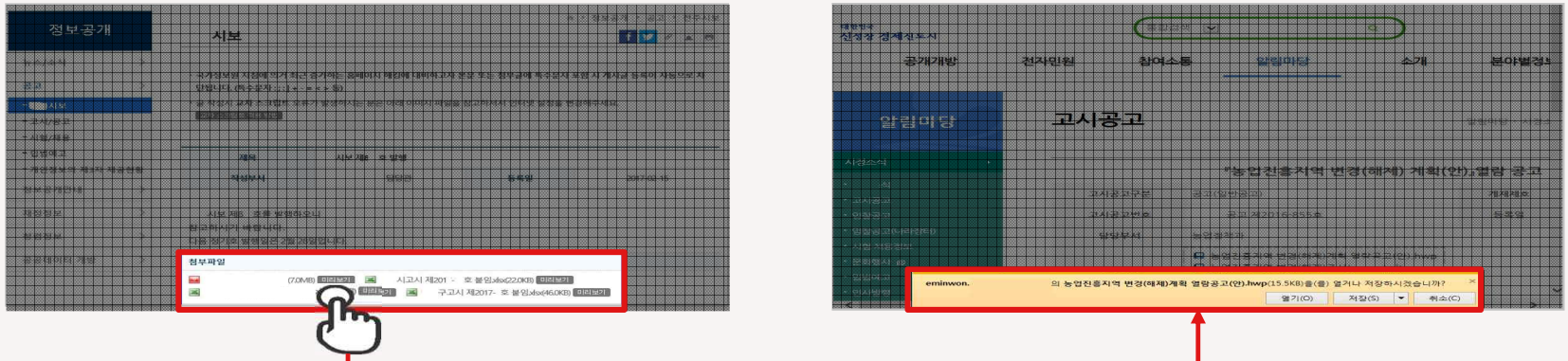
○

6. 홈페이지 노출 사례 ① 첨부 파일에 의한 노출 사례(XLS)

2018년 첨부파일 노출 유형 Top 3



개인정보가 포함된 엑셀 파일을 첨부하여 게시판에 게시

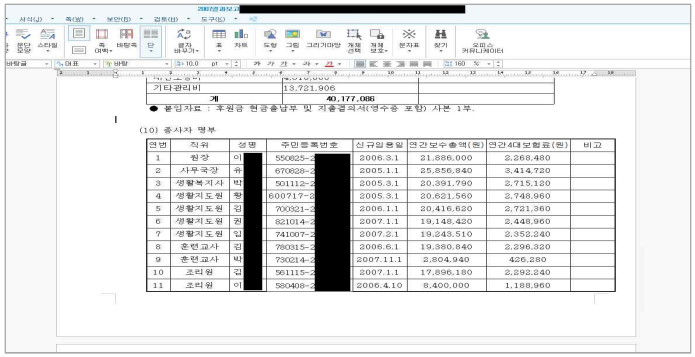


<클릭 시, "저장" 가능>

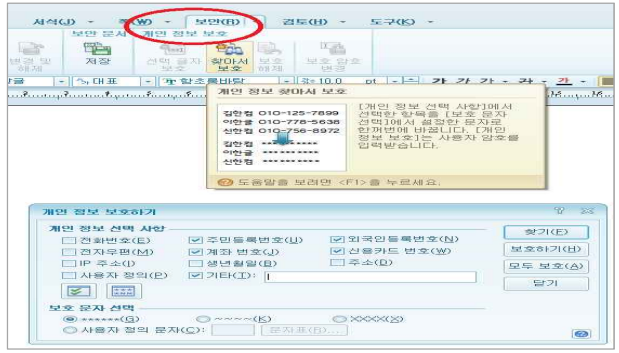
6. 홈페이지 노출 사례 ① 첨부 파일에 의한 노출 사례(HWP, PDF, JPG)

첨부된 한글파일(HWP)에 개인정보 노출

개인정보가 포함된 한글문서

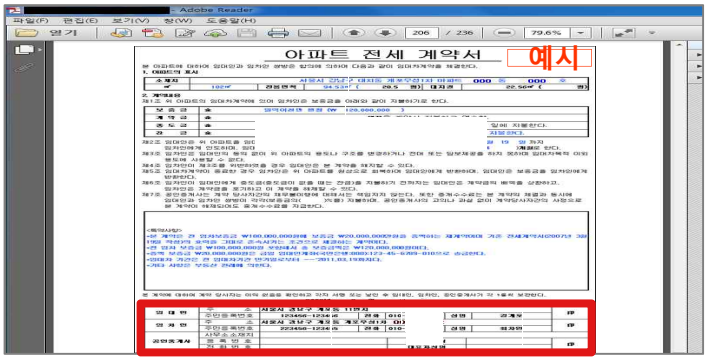


한글의 개인정보 보호 기능을 이용



첨부된 이미지 파일(PDF, JPG 등)에 개인정보 포함

개인정보가 포함된 PDF 이미지



개인정보가 포함된 JPG 이미지

6. 홈페이지 노출 사례 ② 게시글 및 댓글에 의한 노출

여행 상담, 자격증 재발급 요청 등을 하면서 개인정보 노출

개인정보가 포함된 상담 글


Q&A

제 목 재발급 요청

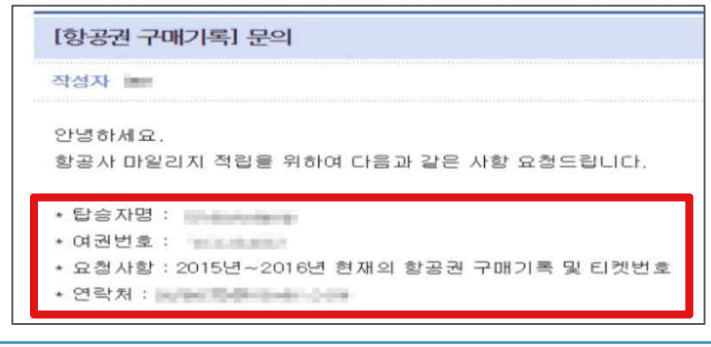
작성자 이

안녕하세요

재발급을 요청드립니다.

발급연도는 20 년 인지 20 년 등증에 한 해이고,
대학교 재학시에 학교에서 시험보고 땄으며,
주민등록번호는 820126- 이고,
연락처는 010-9 입니다.

개인정보가 포함된 게시글

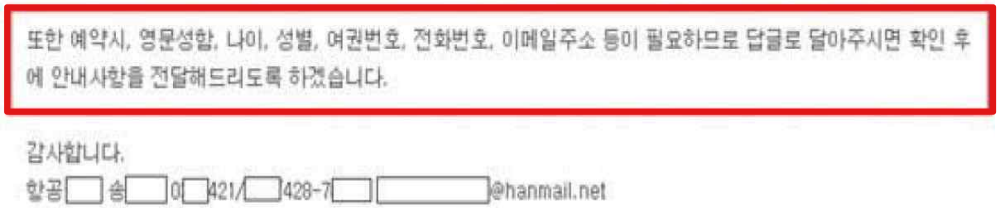

[항공권 구매기록] 문의

작성자

안녕하세요.
항공사 마일리지 적립을 위하여 다음과 같은 사항 요청드립니다.

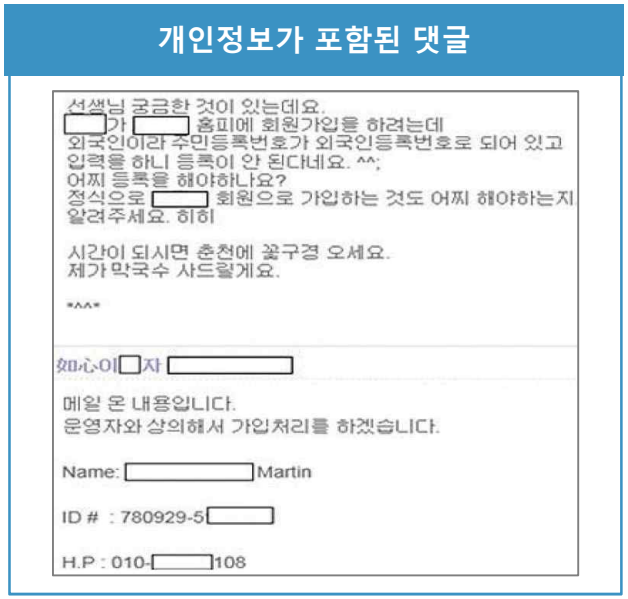
- 탑승자명 :
- 여권번호 :
- 요청사항 : 2015년~2016년 현재의 항공권 구매기록 및 티켓번호
- 연락처 :

공개 게시판 댓글에 개인정보를 남기도록 유도


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

감사합니다.
항공 송 0 421/ 428-7 @hanmail.net

개인정보가 포함된 댓글


선생님 궁금한 것이 있는데요.
가 홈피에 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이 자

메일 온 내용입니다.
운영자와 상의해서 가입처리를 하겠습니다.

Name: Martin

ID # : 780929-5

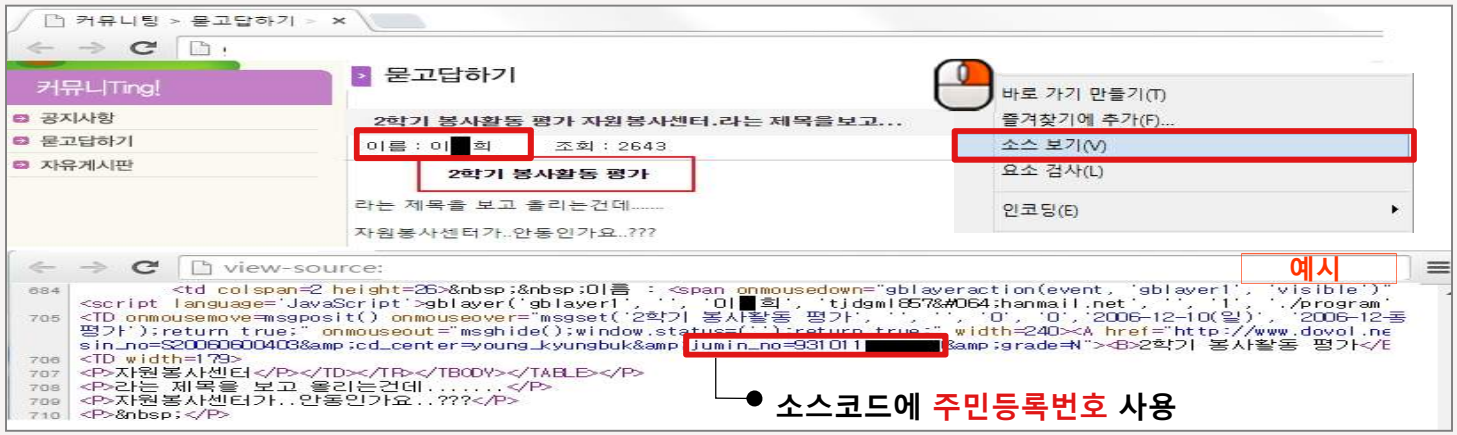
H.P : 010- 108

댓글에 개인정보 노출

저~ 홈페이지 아시죠? 그곳에서 ID는 ***1***, PW는 *********를 치고 들어가세요. 그 다음에는 홍길동이 주민등록번호 900101-4******을 입력하시면 다음 창으로 넘어갑니다.

6. 홈페이지 노출 사례 ③ 홈페이지 설계 및 관리 미흡 (소스코드)

홈페이지 설계 오류로 홈페이지 소스코드에 노출



홈페이지 설계 오류인 디렉터리 리스팅 취약점으로 인해 노출

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

디렉터리 리스팅 올바른 설정 : 윈도우 인터넷 정보서비스(IIS)

- 제어판 > 관리도구 > 인터넷 서비스 관리자 > 기본 웹사이트 속성 정보 수정
  ※ 디렉터리 검색 부분을 비활성화

6. 홈페이지 노출 사례 ③ 홈페이지 설계 및 관리 미흡 (접근제한)

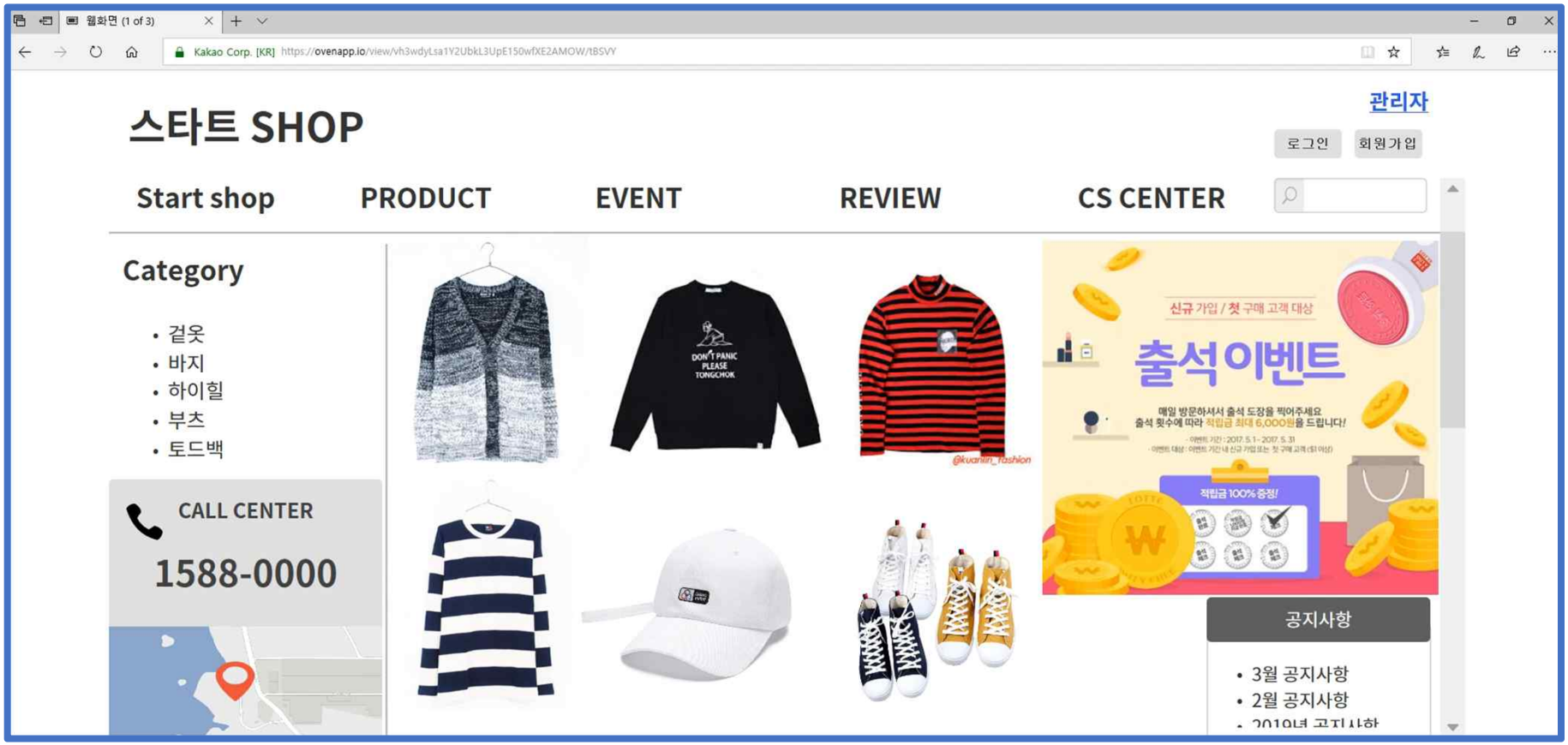
관리자만 볼 수 있는 페이지가 인증 과정을 거치지 않고 방치되어 일반 이용자에게 노출

- LINK 바로가기 삭제
- 유추 가능한 관리자 페이지 주소는 변경
  예시) "/Manager_page", "/admin"・・・등

외부망 검색은 "VPN"이나 "전용망"으로 조치
관리자 페이지는 내부망에서만 검색

인증/세션 정보
작성된 웹 페이지 마다 관리자 "세션" 및 "쿠키" 확인

6. 홈페이지 노출 사례 ③ 홈페이지 설계 및 관리 미흡



7. 기 타

중국내 한국인의 개인정보 불법거래 성행

✓ 프로듀스48 인기투표를 위해 G마켓ID가 중국 오픈마켓(타오바오)에서 거래

✓ 타오바오 등 200여개 중국 사이트 집중 모니터링('18.8)을 통해 탐지, 삭제

KISA 한국인터넷진흥원

Ⅱ. 개인정보유출 후속조치

1. 개인정보 유출 시 법률적 대응방안
2. 개인정보유출 사고 대응 방안

KISA 한국인터넷진흥원

1. 개인정보 유출 시 법률적 대응방안

1 기업 관점

2 피해자 관점

1. 기업 관점

개인정보 침해사고와 위기대응(1/4)

개인정보 유출 통지 의무(개인정보 보호법 제34조 제1항)

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

| 통 지 항 목 |

① 유출된 개인정보의 항목

② 유출 시점과 그 경위

③ 피해 최소화를 위한 정보주체의 조치방법

④ 기관의 대응 조치 및 피해 구제 절차

⑤ 피해 신고 접수 담당부서 및 연락처

| 통 지 방 법 |

① 통지는 서면 등의 방법으로 하여야 함

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

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

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

1. 기업 관점

개인정보 침해사고와 위기대응(1/4)

예 시(1/3)

○○를 믿고 아껴 주시는 회원 여러분

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

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

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

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

1. 기업 관점

개인정보 침해사고와 위기대응(1/4)

예 시(2/3)

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

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

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

1. 기업 관점

개인정보 침해사고와 위기대응(1/4)

예 시(3/3)

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

(⑤ 피해 신고 접수 담당부서 및 연락처)

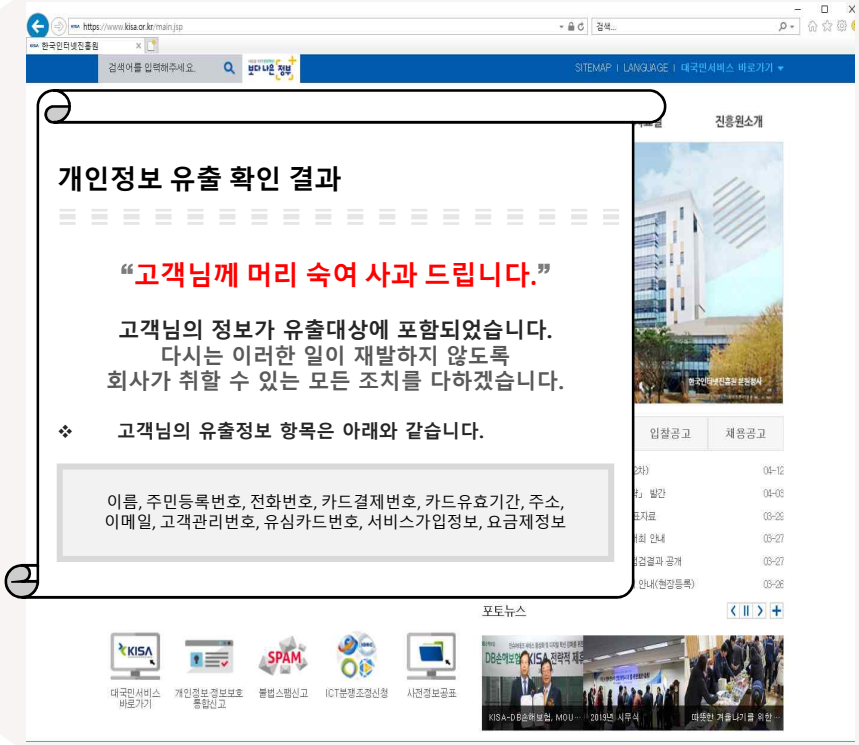
■ 피해 등 접수 담당부서 : ○○ 운영팀
■ 피해 등 접수 전화번호 : 02-2164-1004
■ 피해 등 접수 E-메일주소 : ANGEL@GOD.COM

1. 기업 관점

개인정보 침해사고와 위기대응(2/4)

인터넷 홈페이지 게시(개인정보보호법 시행령 제40조 제3항)

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



|통지사항|

① 유출된 개인정보의 항목

② 유출 시점과 그 경위

③ 피해 최소화를 위한 정보주체의 조치방법

④ 기관의 대응 조치 및 피해 구제 절차

⑤ 피해 신고 접수 담당부서 및 연락처

1. 기업 관점

개인정보 침해사고와 위기대응(3/4)

❖ 개인정보 유출 신고 의무(개인정보보호법 제34조 제3항)

1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 통지 결과 및 조치 결과를 지체없이 행정안전부 또는 전문기관(한국인터넷진흥원)에 신고하도록 하였음

❖ 이용자의 개인정보 유출이 발생한 경우(정통망법)

☞ 유출되었음을 알게 된 후 24시간 이내 해당 이용자에게 개인정보 유출 통지

☞ 방송통신위원회 또는 한국인터넷진흥원(www.i-privacy.kr)에 유출 신고

※ 자세한 사항은 온라인 개인정보보호 포털(www.i-privacy.kr) - 자료실 - 법규 및 지침 – 가이드라인의 '개인정보 유출 대응 매뉴얼'을 참고하시기 바랍니다.

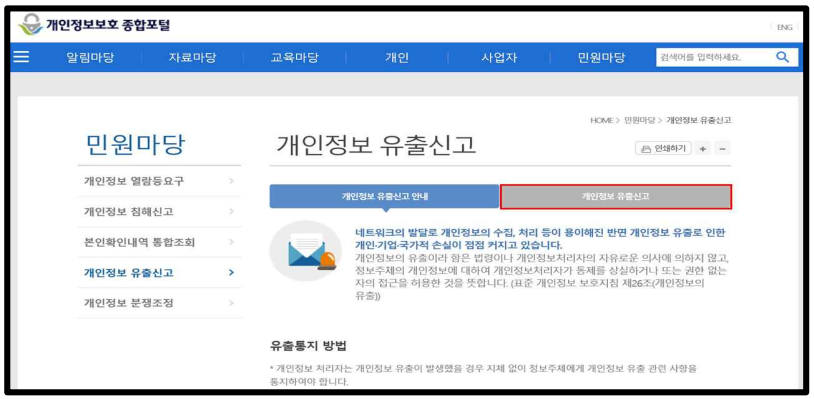
1. 기업 관점

개인정보보호 종합포털(www.privacy.go.kr)을 통한 개인정보 유출 신고 절차

1 개인정보보호 종합포털(www.privacy.go.kr) 접속

2 민원마당 내 '개인정보 유출신고' 클릭

3 개인정보 유출신고 안내사항 확인 후 작성



4 유출신고 작성예시

1. 기업 관점

KISA 온라인 개인정보보호 포털(www.i-privacy.kr)을 통한 개인정보 유출 신고 절차

1 온라인 개인정보보호 포털(www.i-privacy.kr) 접속

2 '개인정보 유출신고'-'개인정보 유출신고하기' 클릭

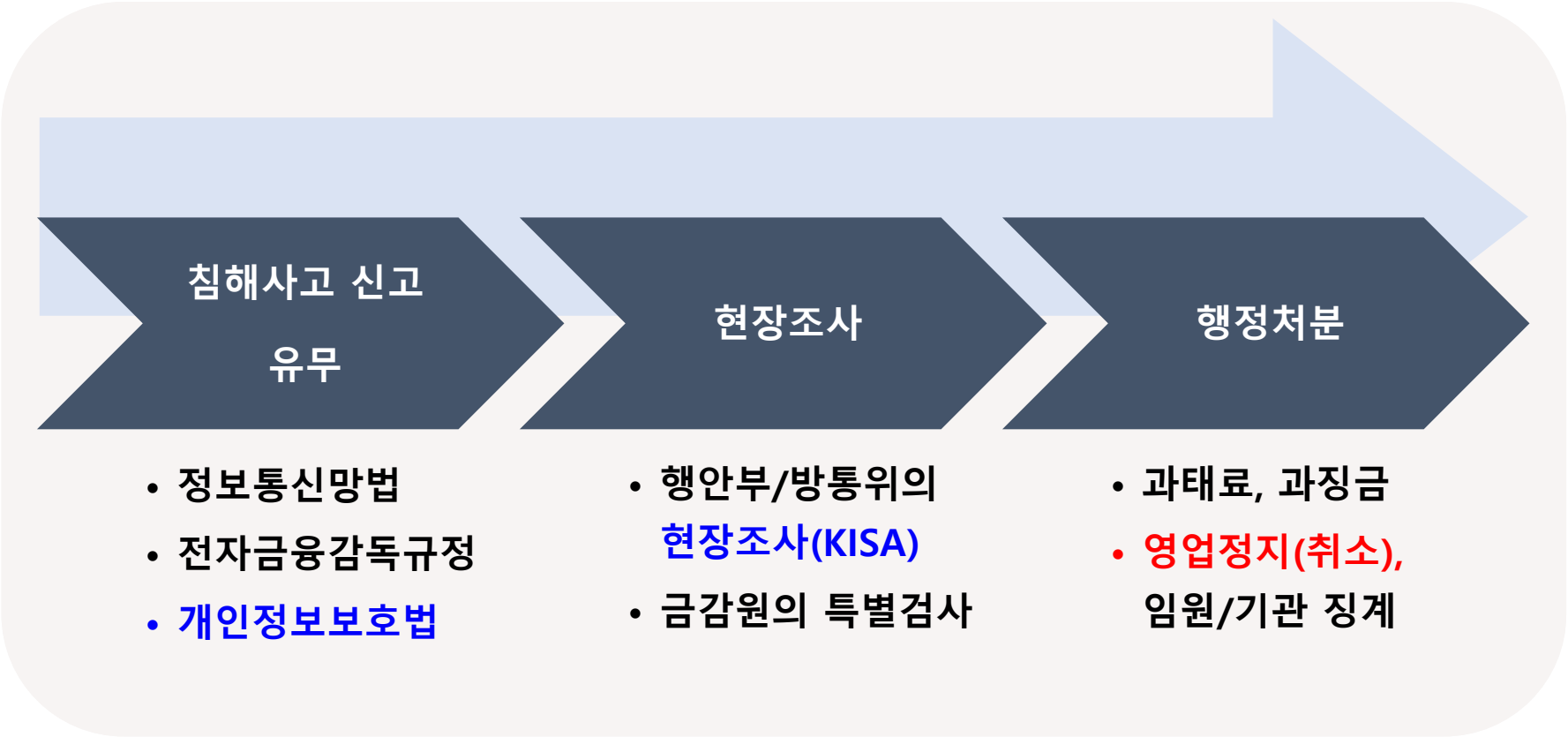
3 유형 선택 후 유출신고서 작성

4 유출신고 작성예시

1. 기업 관점

개인정보 침해사고와 위기대응(4/4)

국가기관의 현장조사 및 행정처분



2. 피해자 관점

개인정보 유출에 대한 서비스 제공자의 책임(2/4)_개인정보보호법

민사책임 [이용자 : '법 위반행위 + 손해'를 입증] [서비스제공자 : '고의·과실 없음'을 입증]

제39조의 2 (법정손해배상의 청구)

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

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

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

[본조신설 2015. 7. 24.]

2. 피해자 관점

개인정보 유출에 대한 서비스 제공자의 책임(1/4)_정보통신망법

민사책임 [이용자 : '법 위반행위 + 손해'를 입증] [서비스제공자 : '고의·과실 없음'을 입증]

제39조(손해배상책임)

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 삭제 <2015. 7. 24.>

③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다. <신설 2015. 7. 24.>

④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015. 7. 24.>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

2. 피해자 관점

개인정보 유출에 대한 서비스 제공자의 책임(3/4)

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

➢ 과징금의 부과

개인정보보호법 제34조의 2

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

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

정보통신망법 제64조의 3

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

(제1항제6호) 이용자의 개인정보를 **분실·도난·유출·위조·변조 또는 훼손한 경우**로서 제28조제1항 제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 **조치를 하지 아니한 경우**

개인정보의 보호조치

(대법원 판례)

과징금부과처분은 원칙적으로 위반자의 고의·과실을 요하지 아니하나, 위반자의 의무 해태를 탓할 수 없는 정당한 사유가 있는 등의 특별한 사정이 있는 경우에는 이를 부과할 수 없다.

2. 피해자 관점

개인정보 유출에 대한 서비스 제공자의 책임(4/4)_개인정보보호법

형사책임 인과 관계 요구함

제73조(벌칙)

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

1. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실・도난・유출・위조・변조 또는 훼손당한 자
2. 제36조제2항을 위반하여 정정・삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

2. 피해자 관점

개인정보 유출에 대한 서비스 제공자의 책임(4/4)_정보통신망법

형사책임 인과 관계 요구함

제73조(벌칙)

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손한 자

1의2. 제29조제1항을 위반하여 개인정보를 파기하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

2. 제42조를 위반하여 청소년유해매체물임을 표시하지 아니하고 영리를 목적으로 제공한 자

3. 제42조의2를 위반하여 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시한 자

이하생략

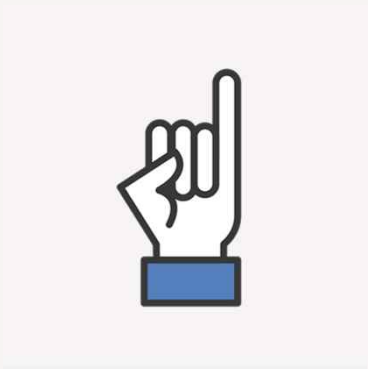
KISA 한국인터넷진흥원

2. 개인정보유출 사고 대응 방안

1. 개인정보 유출·침해사고 대응을 위한 조치
2. 개인정보 안전성 확보조치
3. 개인정보 파기
4. e프라이버시 클린서비스를 통한 개인정보 삭제

1. 개인정보 유출·침해사고 대응을 위한 조치

예방수칙



① 개인정보 최소 수집 및 파기

② 인터넷 게시 전에 다시 한번 문서/홈페이지 확인

③ 관리자페이지는 반드시 보안설정

④ 주기적 점검(내부, 외부)은 필수

개인정보보호법 제29조(안전조치 의무)

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

정보통신망법 제28조(개인정보의 보호조치)

정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

법률에서 정한 최소한의 보호조치

	개인정보의 안정성 확보 조치 기준	개인정보의 기술적 · 관리적 보호조치 기준
적용대상	• 공공기관, 법인, 단체 및 개인 등 개인정보처리자	• 정보통신서비스 제공자
고시근거	• 개인정보보호법 제23조(민감정보의 처리제한)제2항 제24조(고유식별정보의 처리제한)제3항 제29조(안전조치 의무)	• 정보통신망법 제28조(개인정보의 보호조치)
	• 개인정보보호법 시행령 제21조(고유식별정보의 안전성 확보 조치) 제30조(개인정보의 안전성 확보 조치)	• 정보통신망법 시행령 제15조(개인정보의 보호조치)
처벌규정	• 제34조의2(과징금의 부과) 주민등록번호가 유출, 도난 등이 된 경우로서 안전성 확보에 필요한 조치를 하지 않을 경우 5억원 이하 과징금 부과 가능	• 제64조의3(과징금의 부과 등) 이용자의 개인정보를 유출, 도난 한 경우로서 제28조제1항2호부터 5호까지의 조치를 취하지 아니한 경우, 위반행위 관련 매출액의 100분의3 이하에 해당하는 과징금 부과 가능
	• 제73조(벌칙) 안전성 확보조치 기준 위반으로 인하여 개인정보가 유출, 도난, 훼손 등이 된 경우 2년 이하 징역 또는 2천만원 이하 벌금	• 제73조(벌칙) 보호조치 기준 위반으로 인하여 개인정보가 유출, 도난, 훼손 등이 된 경우 2년 이하 징역 또는 2천만원 이하 벌금
	• 제75조(과태료)제2항제6호 위반 시 3천만원 이하 과태료	• 제76조(과태료) 위반시 3천만원 이하 과태료

징벌적 손해배상

2. 개인정보 안전성 확보를 위한 필요 조치

① 내부관리계획의 수립 • 시행

개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음의 사항을 포함하는 내부 관리계획을 수립·시행

내부관리계획 항목

✓ 개인정보 보호책임자의 지정에 관한 사항	✓ 물리적 안전조치에 관한 사항
✓ 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항	✓ 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
✓ 개인정보취급자에 대한 교육에 관한 사항	✓ 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
✓ 접근 권한의 관리에 관한 사항	✓ 위험도 분석 및 대응 방안 마련에 관한 사항
✓ 접근 통제에 관한 사항	✓ 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
✓ 개인정보의 암호화 조치에 관한 사항	✓ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
✓ 접속기록 보관 및 점검에 관한 사항	✓ 그 밖에 개인정보 보호를 위하여 필요한 사항
✓ 악성 프로그램 등 방지에 관한 사항	

위의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리, 개인정보 보호 책임자는 연1회 이상으로 내부관리계획의 이행 실태를 점검·관리

2. 개인정보 안전성 확보를 위한 필요 조치

① 내부관리계획의 수립 • 시행

개인정보 내부 관리계획 작성 예시

Ⅱ 개인정보 내부 관리계획 작성 예시

결재	CEO	실장	부서장

○○○○○ (개인정보처리자명)

개인정보 내부 관리계획

용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

16. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
17. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
18. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(적용 범위) ○○○○○(개인정보처리자명)가 개인정보를 처리하거나 ○○○○○(개인정보처리자명)의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 개인정보 내부 관리계획이 적용된다.

제2장 내부 관리계획의 수립 및 시행

제4조(내부 관리계획의 수립 및 승인) ① 개인정보 보호책임자는 ○○○○○(개인정보처리자명)가 개인정보 보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.

③ 개인정보 보호책임자는 제1항, 제2항에 따라 내부 관리계획을 수립하거나 수정하

개인정보보호 종합포털 → 자료마당 → 참고자료 → 기타 → 개인정보 내부 관리계획

2. 개인정보 안전성 확보를 위한 필요 조치

② 접근권한의 관리(제5조)

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

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

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

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

⑤ 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용

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

2. 개인정보 안전성 확보를 위한 필요 조치

③ 접근통제(제6조)

① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 기본 조치

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

→ 위 기능을 포함하여 조치해야 함

② 외부에서 개인정보처리시스템에 접속하려는 경우안전한 접속수단 또는 안전한 인증수단 적용

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

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

2. 개인정보 안전성 확보를 위한 필요 조치

③ 접근통제(제6조)

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

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

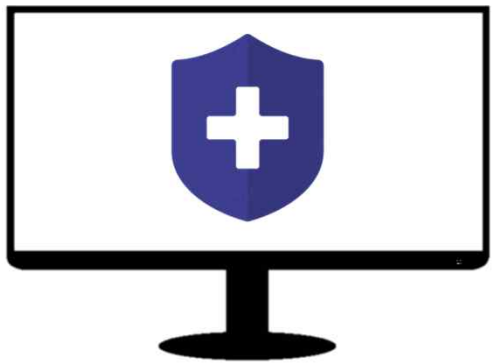
⑥ 별도의 개인정보처리시스템이 아닌 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우

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

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

2. 개인정보 안전성 확보를 위한 필요 조치

④ 관리용 단말기 안전조치(제10조)



관리용 단말기

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

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

② 본래 목적 외로 사용되지 않도록 조치

③ 악성프로그램 감염 방지 등을 위한 보안 조치 적용

고려사항

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

2. 개인정보 안전성 확보를 위한 필요 조치

⑤ 개인정보 암호화(제7조)

암호화 필요 대상

고유식별정보
비밀번호
바이오정보

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

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

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

2. 개인정보 안전성 확보를 위한 필요 조치

⑥ 개인정보 암호화(제7조)_ 암호화 기준

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

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

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

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

2. 개인정보 안전성 확보를 위한 필요 조치

⑦ 접속기록의 보관 및 점검(제8조)

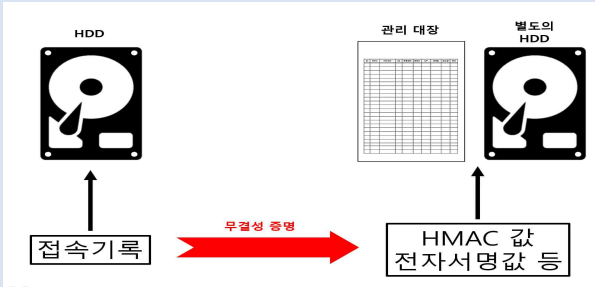
① 개인정보 취급자가 개인정보처리시스템에 접속한 기록을(6개월-> 1년) 이상 안전하게 보관・관리(5만명이상 2년)

② 개인정보처리시스템의 접속기록 등을 (반기별로 1회->월1회) 이상 점검(개정예정)

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

접속기록 항목 (예시)				
취급자 식별정보	정보주체 식별정보	접속일시	접속지	수행업무
홍길동	성춘향	20XX.04.18 15:00:00	172.168.11.11	노출교육 신청

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



2. 개인정보 안전성 확보를 위한 필요 조치

⑧ 악성프로그램 방지(제9조)

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

① 보안 프로그램은 항상 최신의 상태로 유지

- 자동 업데이트 기능 사용
- 일 1회 이상 업데이트 실시

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

③ 발견된 악성 프로그램 등에 대해 삭제 등 대응 조치

2. 개인정보 안전성 확보를 위한 필요 조치

⑨ 물리적 안전조치(제11조)

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

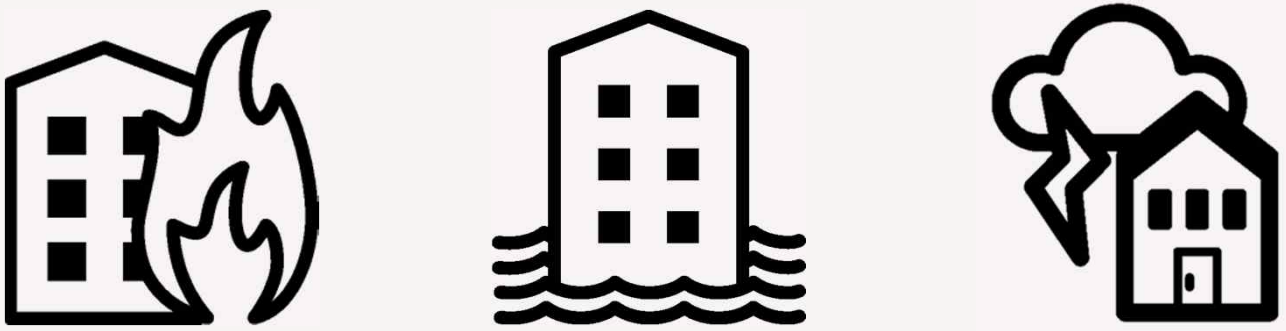
② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관

③ 개인정보가 포함된 보조저장매체의 반출.입 통제를 위한 보안대책을 마련

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

2. 개인정보 안전성 확보를 위한 필요 조치

⑩ 재해 • 재난 대비 안전조치(제12조)



화재, 홍수, 단전 등의 재해. 재난 발생 시

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

② 개인정보처리시스템 백업 및 복구를 위한 계획 마련

3. 개인정보파기(제13조)

전체 파기

① 개인정보 파기 조치

완전파괴
(소각·파쇄 등)

전용 소자장비
이용하여 삭제

데이터가 복원
되지 않게 초기화
또는 덮어쓰기

일부 파기

② 1항의 방법이 어려울 경우 일부 파기 조치

전자적 파일 형태인 경우

개인정보를 삭제한 후 복구 및
재생되지 않도록 관리 및 감독

**제1호 외의 기록물, 인쇄물,
서면, 그 밖의 기록매체인 경우**

해당 부분을 마스킹, 천공 등으로 삭제

[참고] 개인정보 침해신고센터 업무 절차

개인정보·정보보호
통합신고
(KISA.or.kr / ☎118)

민원접수

신고/상담
법령질의 구분

일반상담

상담 후 종결
(형사벌 사안 등)

법령질의

신고접수

검토의견 작성

사실조사

답변 후 종결

관련부처 검토

민원처리심사위원회

심의

사실조사
결과보고서 작성

법 위반 사실이 있는 경우

관련부처
(행정처분)

국민은 개인정보 보호 실천 생활화

개인정보 오남용 피해 방지 10계명

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

❖ 개인정보 침해신고 적극 활용하기

개인정보가 유출된 경우 즉시 개인정보 침해신고하기

☞ privacy.kisa.or.kr

❖ 개인정보처리방침 및 이용약관 꼼꼼히 살피기

개인정보 처리자는 개인정보 취급 관련 내용을 개인정보처리방침에 포함하여 공개해야함

❖ 비밀번호는 문자와 숫자로 8자리 이상

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

❖ 비밀번호는 주기적으로 변경하기

자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 주기적으로 비밀번호 변경

❖ 회원가입은 주민번호 대신 I-PIN 사용

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

❖ 명의도용확인 서비스 이용하여 가입정보 확인

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

❖ 개인정보는 친구에게도 알려주지 않기

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

❖ P2P공유폴더에 개인정보 저장하지 않기

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

❖ 금융거래는 PC방에서 이용하지 않기

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

❖ 출처가 불명확한 자료는 다운로드 금지

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

개인정보 유 · 노출

질/의/응/답

KISA 한국인터넷진흥원

Internet On, Security In!

Thank you

개인정보보호 종합포털 www.privacy.go.kr

e프라이버시 클린서비스 www.eprivacy.go.kr

개인정보침해신고센터 (국번없이) 118

(홈페이지) privacy.kisa.or.kr