개인정보 유출 대응 매뉴얼

2020. 12.

개인정보보호위원회

◇ 본 매뉴얼은 「개인정보 보호법」제34조, 제39조의4 및 「신용정보의 이용 촉진 및 보호에 관한 법률」(이하 ‘신용정보법) 제39조의4에 따라 ‘개인정보보호위원회’ 또는 ‘한국인터넷진흥원’에 신고하여야 하는 개인정보 유출 사고와 관련하여 신속한 대응과 그 피해를 최소화하기 위한 최소한의 사항을 안내하고 있습니다.

- 처리하는 개인(신용)정보의 종류, 처리하는 방법 및 환경, 사고 유형 및 규모 등에 따라 다르게 적용될 수 있으므로 스스로의 환경을 고려하여 “개인정보 유출 대응 매뉴얼”을 마련하여야 합니다.

목 차

Ⅰ 개인정보 유출 개요

1. 개인정보 유출이란?

o 개인정보의 유출은 “표준 개인정보 보호지침” 제25조에 따라 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 말합니다.

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

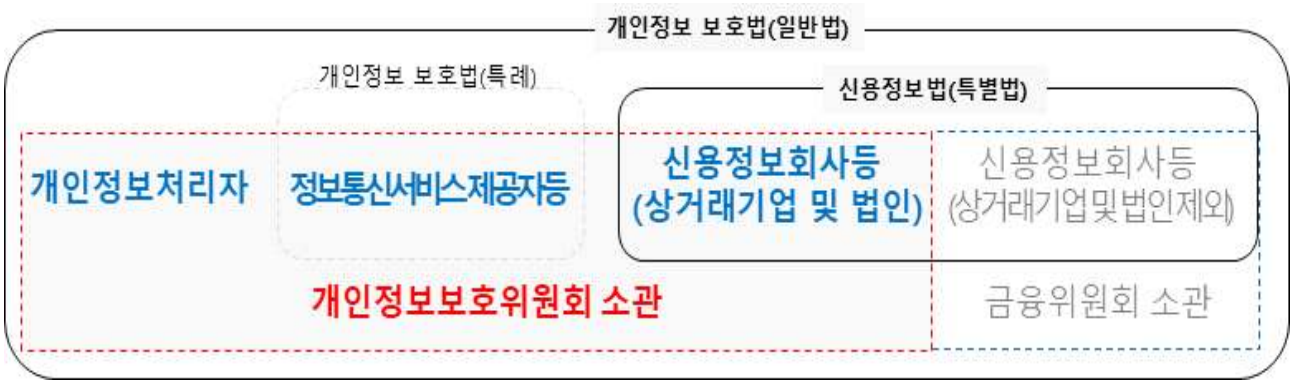
※ 신용정보법 제39조의4에 따른 “누설”을 포함

2. 법률과의 관계 및 적용 범위

o 개인정보처리자가 개인정보를 유출한 경우에는 「개인정보 보호법」 제34조가 적용됩니다. 다만, 정보통신서비스 제공자등은 「개인정보 보호법」 제39조의4가, 신용정보회사등(상거래기업 및 법인)은 「신용정보법」 제39조의4가 우선 적용됩니다.

※ 신용정보회사등(상거래기업 및 법인) : “개인정보보호위원회등”에 신고
신용정보회사등(상거래기업 및 법인을 제외한 전체) : “금융위원회등”에 신고

< 개인정보 유출 관련 법 체계 >



< 개인정보 유출 관련 법 적용 비교 >

근거 법률		개인정보 보호법		신용정보법
		제34조(개인정보 유출 통지 등)	제39조의4(개인정보 유출등의 통지·신고 특례)	제39조의4(개인신용정보 누설통지 등)
법률간의 관계		일반법	일반법(특례)	특별법
적용 대상		개인정보처리자	정보통신서비스 제공자등	신용정보회사등에서의 상거래기업 및 법인에 한정
적용 범위		개인정보 유출	개인정보 분실·도난·유출	개인신용정보 누설
의무 사항		통지 및 신고		
벌칙 규정		3천만원 이하의 과태료		
유출신고	규모	1천명 이상	1명 이상	1만명 이상
	시점	5일 이내	24시간 이내	5일 이내
	기관	개인정보보호위원회 또는 한국인터넷진흥원		
유출통지	규모	1명 이상		
	시점	5일 이내	24시간 이내	5일 이내
	방법	홈페이지, 전화, 팩스, 이메일, 우편 등으로 개별 통지		
	항목	유출된 개인정보 항목, 유출된 시점과 그 경위, 정보주체 피해 최소화 조치, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처 등		

Tip

▶ 개인정보 : 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)

▶ 개인신용정보 : 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보

나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보

▶ 개인정보처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

▶ 정보통신서비스 제공자등 : 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자

- 정보통신서비스 제공자 : 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

▶ 신용정보회사등 : 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 신용정보제공·이용자

- 신용정보회사, 본인신용정보관리회사 등은 신용정보법 제2조(정의) 참조

▶ 상거래기업 및 법인 : 금융위원회의 감독을 받지 아니하는 신용정보제공·이용자

3. 법적 의무사항

1 개인정보 유출 사고 대응 계획 수립·시행

o “개인정보 유출 사고 대응 계획”에 관한 사항을 내부 관리계획에 포함하여 수립·시행하여야 합니다.

※ 근거 : 「개인정보 보호법」 제29조 및 동법 시행령 제30조, “개인정보의 안전성 확보조치 기준” 제4조제1항제11호 및 “개인정보의 기술적·관리적 보호조치 기준 제3조제1항제6호

2 개인정보 유출 사고 대응 매뉴얼 마련

o 개인정보 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 공공기관 및 1만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자는 “개인정보 유출 사고 대응 매뉴얼”을 마련하여야 합니다.

※ 근거 : 「개인정보 보호법」 제12조, “표준 개인정보 보호지침” 제29조제1항

3 개인정보 유출 통지 및 신고

o 개인정보가 유출되었음을 알게 되었을 때에는 해당 정보주체에게 유출사실을 통지하여야 합니다.

o 또한, 일정규모 이상의 정보주체가 유출된 경우에는 유출 통지 결과 및 유출로 인한 피해 최소화를 위해 조치한 결과를 지체 없이 개인정보보호위원회 또는 한국인터넷진흥원에 신고하여야 합니다.

※ 근거 : 「개인정보 보호법」 제34조 및 제39조의4, 동법 시행령 제39조, 40조, 제48조의4, “표준 개인정보 보호지침” 제26조부터 제28조 그리고 「신용정보법」 제39조의4 및 동법 시행령 제34조의4, 신용정보업감독규정 제43조의5, 제43조의6

< 개인정보 유출 대응 절차 [요약] >

Ⅰ 유출 대응체계 구축

CEO 의사결정

개인정보유출 신속대응팀

개인정보보호 책임자
- 개인정보 유출 대응 총괄 지휘
- 개인정보 유출대응 신속대응팀 구성·운영

개인정보보호 담당자
- 유관기관에 개인정보 유출 신고
- 이용자에게 개인정보 유출 통지

정보보호 담당자
- 유관기관에 침해사고 신고
- 사고경위 분석, 시스템 복구 등 침해대응

고객지원 부서
- 정부, 언론사, 이용자 민원 대응
- 이용자 피해구제 및 분쟁조정 기구 안내

Ⅱ 피해 최소화 및 긴급 조치

해킹	시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경 등
내부자	유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력물 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등
이메일	발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일 서버 운영자에게 파일 삭제 요청, 파일 전송시 암호화 등
노출	• 검색엔진 : 노출된 개인정보 삭제 요청, 로봇배제 규칙 적용 등 • 시스템 오류 : 소스 코드, 서버 설정 등 원인 파악 및 수정 등 • 홈페이지 게시 : 게시글 삭제, 첨부파일에서 개인정보 마스킹 등

Ⅲ 유출 통지 및 신고

적용 대상		개인정보처리자	정보통신서비스 제공자등	신용정보회사등에서의 상거래기업 및 법인에 한정
유출 신고	규모	1천명 이상	1명 이상	1만명 이상
	시점	5일 이내	24시간 이내	5일 이내
	기관	개인정보보호위원회 또는 한국인터넷진흥원		
유출 통지	규모	1명 이상		
	시점	5일 이내	24시간 이내	5일 이내
	방법	홈페이지, 전화, 팩스, 이메일, 우편 등으로 개별 통지		
	항목	유출된 개인정보 항목, 유출된 시점과 그 경위, 정보주체 피해 최소화 조치, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처 등		

Ⅳ 피해 구제 및 재발 방지

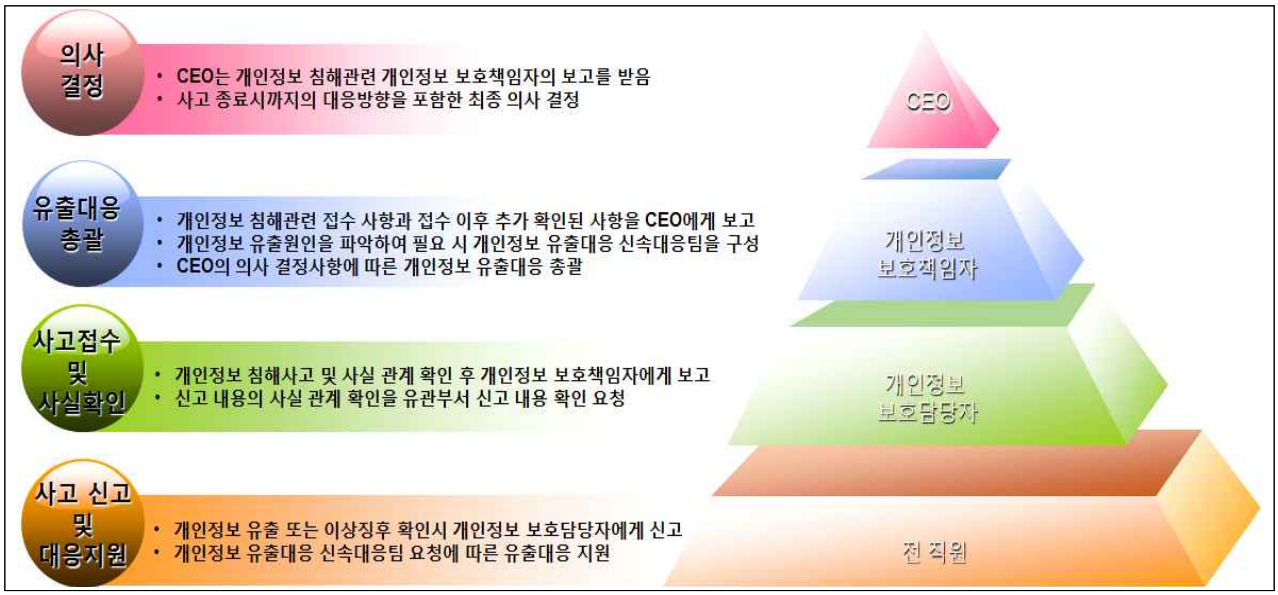
정보주체 피해 구제
- 홈페이지 등을 통한 유출여부 조회 기능 제공
- 유출로 인한 피해 신고, 접수, 상담, 문의 등 각종 민원대응 방안 마련
- 유출 대응 현장 혼란 최소화 방안 강구
- 보이스피싱 등 2차 피해 방지를 위한 유의 사항 안내
- 피해 보상 계획 마련 및 관련 제도 안내 등

재발 방지 대책 마련
- 개인정보 유출 원인 등에 대한 개선방안 마련
- 취급자 대상 개인정보보호 교육 실시
- 홈페이지 취약점 제거 등 개인정보 안전조치 강화 등

Ⅱ 개인정보 유출 대응체계 구축

◇ 개인정보 유출 사실을 알게 된 경우, 개인정보 보호책임자는 즉시 CEO에게 보고하고 개인정보보호·정보호호 부서 등을 중심으로 “개인정보 유출 대응 신속대응팀” 등을 구성하여 피해 확산 방지 및 최소화를 위한 조치를 강구하도록 합니다.

1. 개인정보 유출사실 CEO 보고



o (전직원) 개인정보 유출사실을 발견하거나 의심스러운 정황을 알게된 경우에는 즉시 개인정보보호 담당자에게 전화, 이메일 등으로 신고합니다.

o (개인정보 보호담당자) 신고를 받은 즉시 관계인에게 유출 규모, 경로 등 유출 사실 여부를 확인 요청하고, 개인정보 보호책임자에게 유출 사실 및 피해 규모, 대응 상황 등을 신속하게 보고하여야 합니다.

o (개인정보 보호책임자) 해당 시점까지 파악된 현황을 CEO에게 신속하게 보고하고 새로운 상황이 발생될 때마다 수시로 보고해야 하며, 개인정보 유출이 확인되는 즉시 “개인정보 유출 신속대응팀(T/F)”을 운영합니다.

o (CEO) “개인정보 유출 신속대응팀”을 중심으로 유관부서가 유기적으로 대응하도록 지원하고 유출 대응에 대한 방향성 제시 등 의사결정을 진행합니다.

2. 개인정보 유출 신속대응팀 구성·운영

o “개인정보 유출 신속대응팀”(가칭)을 운영하여 개인정보 유출 사고 발생에 따른 사고 분석, 처리, 사후 복구 및 예방 조치 등을 수행합니다.

- 개인정보 보호책임자를 중심으로 내부 조직 및 인력을 효율적으로 분배하여 유출원인 분석 및 대응, 유출신고·통지, 이용자 피해구제 등 고객지원 등으로 세분화하여 신속히 대응

<table>
<tr><td colspan="3">CEO 의사 결정</td></tr>
<tr><td rowspan="4">개인정보
유출
신속대응팀</td><td>개인정보 보호책임자</td><td>· 개인정보 유출 대응 총괄 지휘
· 개인정보 유출대응 신속대응팀 구성·운영</td></tr>
<tr><td>개인정보 보호담당자</td><td>· 유관기관에 개인정보 유출 신고
· 이용자에게 개인정보 유출 통지</td></tr>
<tr><td>정보보호 담당자</td><td>· 유관기관에 침해사고 신고
· 사고경위 분석, 시스템 복구 등 침해대응</td></tr>
<tr><td>고객지원 부서</td><td>· 정부, 언론사, 이용자 민원 대응
· 이용자 피해구제 및 분쟁조정 기구 안내</td></tr>
<tr><td>전직원</td><td colspan="2">· 개인정보 유출 확인 시 부서장 또는 개인정보보호 부서에 신고
· 침해사고 발생 확인 시 부서장 또는 정보보호 부서에 신고
· 개인정보 유출 신속대응팀 요청에 따른 유출대응 지원</td></tr>
</table>

Ⅲ 피해 최소화 및 긴급 조치

◇ 개인정보 유출 원인을 파악한 후, 피해 최소화 등을 위해 취약점 제거 등 유출 원인을 제거하는 긴급 대응 조치를 실시하도록 합니다.

1 해킹에 의한 경우

o 해킹 등 침해사고 발생으로 인해 개인정보가 유출된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구하여야 합니다.

- 유출된 시스템 분리·차단 조치, 관련 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경* 등 기술적 보호조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급 조치를 시행하여야 합니다.

  * 일방향 암호화되지 않은 비밀번호가 유출되었거나, 해커 등이 이용자의 비밀번호를 알고 있다고 판단되는 경우에는 이용자가 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방 방지

- 사고원인 조사 등이 완료된 이후에는 개인정보 유출의 직·간접적인 원인을 즉시 제거하고, 취약점 개선 조치 등을 수행하여야 합니다.

  ※ 세부내용은 부록3 참고

Tip	▸ 내부 인력의 전문성 부족 등으로 긴급 조치 등이 어려운 경우에는 한국인터넷진흥원에 기술지원을 요청할 수 있습니다. - 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속 권한 삭제·변경 또는 폐쇄 조치 지원 - 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 조치 지원 - 향후 수사 등에 필요한 접속기록 등 증거 보존 조치 지원 등

2 내부자가 유출한 경우

o 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역을 확인하여야 합니다.

o 개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등이 정상적인지 여부 등을 확인하고, 비정상적인 접속인 경우 우회 경로를 확인하여 접속을 차단하여야 합니다.

o 개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출 여부를 확인하여야 합니다.

o 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 필요시 수사기관 등과 협조하여 유출된 개인정보를 회수하기 위한 방법을 강구하여야 합니다.

3 이메일 오발송에 의한 경우

o 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청하도록 합니다.

o 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일서버 운영자에게 관련 파일의 삭제를 요청하여야 합니다.

4 개인정보 노출에 의한 경우

o (검색엔진을 통한 노출의 경우) 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 인증 절차 추가 및 로봇배제 규칙 적용 등 외부 접근을 차단하여야 합니다.

o (시스템 오류로 인한 노출의 경우) 소스코드 오류, 서버 설정 오류 등 개인정보가 노출된 원인이 된 시스템 오류를 파악하여 수정하여야 합니다.

o (개인정보취급자 부주의로 인한 노출의 경우) 게시글 및 첨부파일 내 개인정보 노출 부분을 마스킹 처리하여 게시하도록 합니다.

Ⅳ 개인정보 유출 통지 및 신고

◇ 개인정보 유출 사실을 알게 된 경우에는 정보주체에게 유출사실을 통지하고 개인정보보호위원회 또는 한국인터넷진흥원에 유출 사실을 신고하여야 합니다.

1. 개인정보 유출 통지

o (통지 주체) 개인정보를 처리하는 "개인정보처리자", "정보통신서비스 제공자등" 그리고 개인신용정보를 처리하는 "신용정보회사등"에서의 상거래기업 및 법인이 해당합니다.

근거 법률	개인정보 보호법		신용정보법
	제34조(개인정보 유출 통지 등)	제39조의4(개인정보 유출등의 통지·신고 특례)	제39조의4(개인신용정보 누설통지 등)
통지 주체	개인정보처리자	정보통신서비스 제공자등	신용정보회사등에서의 상거래기업 및 법인에 한정

o (통지 시점) 최초 개인정보의 유출 사실을 알게 되었을 때로부터의 통지 시점을 말합니다.

- 단, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위해 긴급한 조치가 필요하다고 인정되는 경우에는 해당 조치를 취한 후 그로부터 5일 이내에 정보주체에게 알릴 수도 있습니다.

※ 긴급 조치가 필요한 경우에는 반드시 관계 기관과 사전 협의가 필요합니다. 긴급조치가 필요하다고 인정되지 않는 경우에는 3천만원 이하의 과태료가 부과될 수 있습니다.

근거 법률	개인정보 보호법		신용정보법
	제34조	제39조의4	제39조의4
통지 시점	5일 이내 (긴급 조치 가능)	24시간 이내	5일 이내 (긴급 조치 가능)

※ 개인정보 유출 사고를 인지하지 못해 유출 통지가 지연된 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 합니다.

o (통지 규모) 단 1명의 정보주체에 관한 개인정보가 유출된 경우라 할지라도 해당됩니다.

o (통지 방법) 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법으로 개별 통지하는 것을 말합니다.

- 단, 법에서 정한 일정규모 이상의 정보주체에 관한 개인정보가 유출된 경우에는 해당 법에서 정한 방법으로 통지하여야 합니다.

근거 법률	개인정보 보호법		신용정보법
	제34조	제39조의4	제39조의4
통지 방법	1명 이상 : 홈페이지, 전화, 팩스, 이메일, 우편 등		
	(1천명 이상의 경우에는 서면등의 방법과 동시에, 홈페이지 또는 사업장에 7일 이상 게시)	(이용자의 연락처를 알 수 없는 등의 경우에는 홈페이지에 30일 이상 게시)	(1만명 이상의 경우에는 홈페이지 또는 사업장에 15일 이상 게시 또는 신문 등에 7일 이상 게시)

※ 홈페이지에 게시할 때에는 '개인정보 유출 안내', '사과문' 등의 제목을 사용하고, 법에서 정한 통지 내용이 모두 포함되어야 합니다.

- 대규모 유출로 24시간 이내 전체 통지가 기술적으로 불가능한 경우에는 홈페이지 팝업창 등을 통해 방문하는 이용자가 모두 알 수 있도록 현재까지 파악된 유출사실 등을 게시를 하고 나서 추가적으로 해당 정보주체에게 개별적으로 통지를 하여야 합니다.

Tip

▸ 유출 통지를 할 때에는 정보주체가 실제 확인 가능하도록 이용 빈도가 높은 방법을 우선 활용하여 통지하는 것이 바람직합니다.

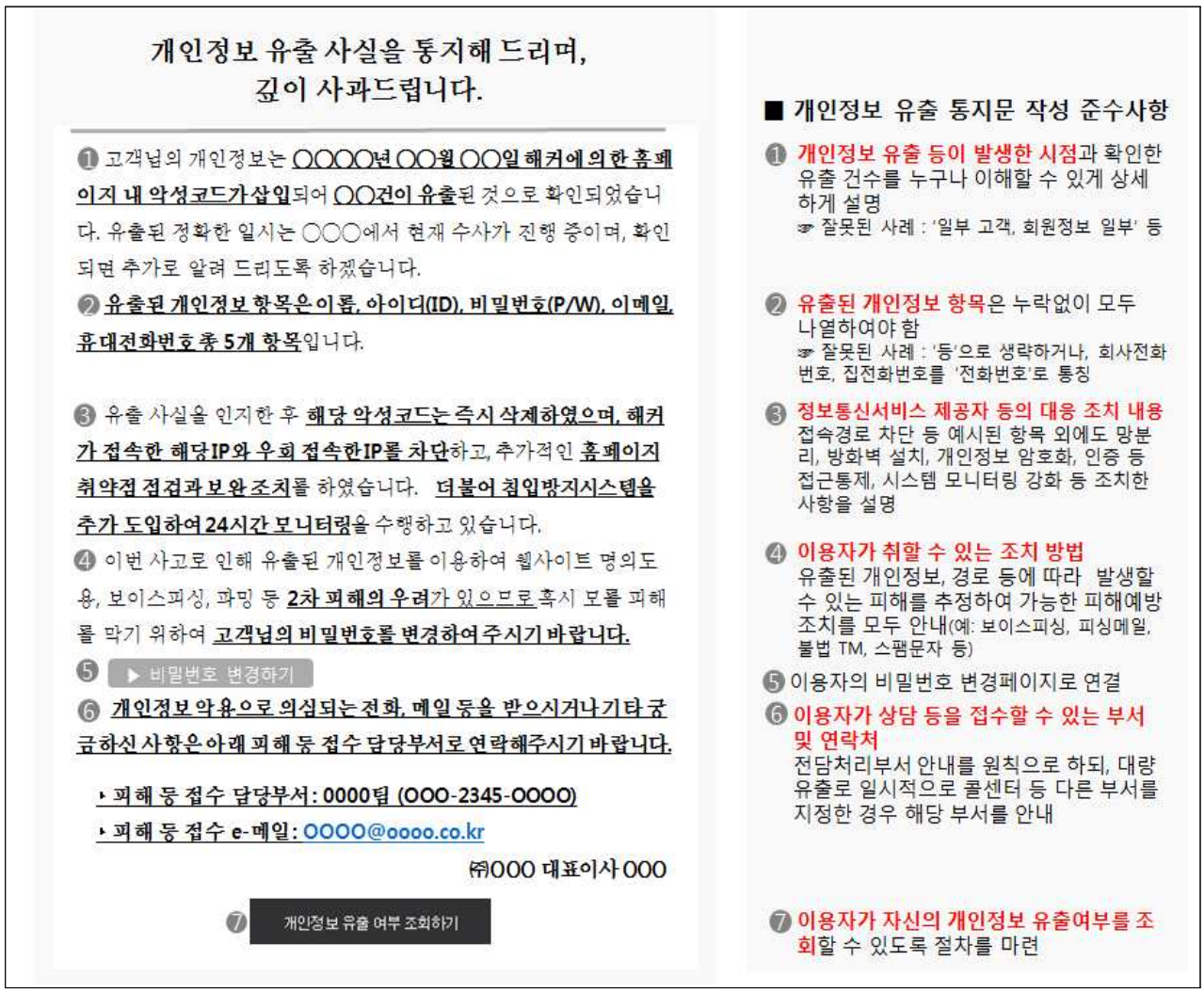
- 휴대전화번호를 보유하고 있는 경우에는 전화통화 및 문자 등을 활용하고 곤란한 경우에는 이메일, 팩스, 우편 등의 방법을 활용

o (통지 내용) ① 유출된 개인정보 항목, ② 유출된 시점과 그 경위, ③ 정보주체가 취할 수 있는 피해 최소화 조치, ④ 개인정보처리자 대응조치 및 피해 구제절차, ⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처 등을 통지해야 합니다.

- 유출 통지하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 통지하고, 추가로 확인되는 내용은 확인되는 즉시 통지하여야 합니다.

※ 구체적 사실관계 파악을 이유로 정보주체에게 유출 사실 통지를 지연하는 경우에는 3천만원 이하의 과태료가 부과될 수 있습니다.

< 홈페이지 개인정보 유출 통지문(예시) >



개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.

❶ 고객님의 개인정보는 **○○○○년 ○○월 ○○일 해커에 의한 홈페이지 내 악성코드가삽입**되어 **○○건이 유출**된 것으로 확인되었습니다. 유출된 정확한 일시는 ○○○에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.

❷ **유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목**입니다.

❸ 유출 사실을 인지한 후 **해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당IP와 우회 접속한IP를 차단**하고, 추가적인 **홈페이지 취약점 점검과 보완 조치**를 하였습니다. **더불어 침입방지시스템을 추가 도입하여 24시간 모니터링**을 수행하고 있습니다.

❹ 이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 파밍 등 **2차 피해의 우려**가 있으므로 혹시 모를 피해를 막기 위하여 **고객님의 비밀번호를 변경하여 주시기 바랍니다.**

❺ ▶ 비밀번호 변경하기

❻ **개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해주시기 바랍니다.**

- **피해 등 접수 담당부서: 0000팀 (000-2345-0000)**
- **피해 등 접수 e-메일: 0000@0000.co.kr**

㈜000 대표이사 000

❼ 개인정보 유출 여부 조회하기

■ 개인정보 유출 통지문 작성 준수사항

❶ **개인정보 유출 등이 발생한 시점**과 확인한 유출 건수를 누구나 이해할 수 있게 상세하게 설명
☞ 잘못된 사례 : '일부 고객, 회원정보 일부' 등

❷ **유출된 개인정보 항목**은 누락없이 모두 나열하여야 함
☞ 잘못된 사례 : '등'으로 생략하거나, 회사전화번호, 집전화번호를 '전화번호'로 통칭

❸ **정보통신서비스 제공자 등의 대응 조치 내용**
접속경로 차단 등 예시된 항목 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명

❹ **이용자가 취할 수 있는 조치 방법**
유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱메일, 불법 TM, 스팸문자 등)

❺ 이용자의 비밀번호 변경페이지로 연결

❻ **이용자가 상담 등을 접수할 수 있는 부서 및 연락처**
전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

❼ **이용자가 자신의 개인정보 유출여부를 조회**할 수 있도록 절차를 마련

잘못된 대응 사례 #1

▸ OO정보통신사는 해킹으로 추정되는 이상 징후를 인지하고 5일 후, 개인정보 유출사실을 확인하고 2일 후부터 유출 통지를 실시함

⇒ 해킹 침해사고로 추정되는 이상 징후를 알게 된 경우에는 관계 기관(과학기술정보통신부 또는 한국인터넷진흥원)에 침해신고를 해야 하고, 개인정보가 유출된 사실을 알게 된 경우에는 24시간 이내에 해당 정보주체에게 개인정보 유출 통지를 이행하여야 함

잘못된 대응 사례 #2

▸ OO사는 해커에 의해 개인정보가 유출된 사실을 확인한 후 경찰청에 신고하였으나, 수사관으로부터 해커가 검거될 때까지는 유출 통지를 유보해 달라는 구두 요청을 받고 30일 이상 통지를 지연

⇒ 해커 검거를 통해 유출된 개인정보를 회수하기 위해 경찰청으로부터 필요한 최소한의 기간 동안 유출 통지 보류를 요청받은 경우에는 개인정보보호위원회에 유출 신고 후 협의하여야 하고 사유를 소명하여야 함

잘못된 대응 사례 #3

▸ OO사는 개인정보 유출 사실을 알게 된 후 유출된 정보주체를 대상으로 유출 통지를 실시하였으나, '아이디', '아이디+일방향 암호화된 비밀번호'만 유출된 이용자에 대하여는 별도의 통지절차를 이행하지 않음

⇒ 유출된 개인정보의 유형이 '아이디+비밀번호'만이더라도 별도로 분리 보관되어 있는 연락처 정보 등을 활용하여 유출 통지를 진행해야 하고, 연락처가 없는 경우에는 홈페이지를 통해 30일 이상 게시하여야 함

잘못된 대응 사례 #4

▸ OO정보통신사는 개인정보취급자가 정보주체 10여명의 인적사항이 담긴 개인정보파일을 이메일에 첨부하여 다른 사람에게 잘못 보냈으나, 해당 파일에 담긴 이용자에게 별도의 유출 통지 절차를 이행하지 않음

⇒ 단 1명의 개인정보라 할지라도 유출되는 경우에는 통지·신고하여야 함

잘못된 대응 사례 #5

▸ OO사는 개인정보 유출을 알게 된 후 자사 홈페이지를 통해 정보주체가 자신의 개인정보가 유출되었는지 여부를 확인하는 페이지를 운영하였으나 본인확인을 위해 이름과 주민등록번호를 입력하도록 하고, 전송구간 암호화 조치를 취하지 않음

⇒ 유출된 정보를 활용하여 본인을 확인하고 전송구간 암호화 미조치로 인하여 추가적으로 개인정보 유출이 발생할 위험성이 존재하므로 주민등록번호 등 유출된 정보를 재활용하지 않도록 하고 전송구간 암호화 조치(보안서버 구축 등)를 반드시 이행하여야 함

2. 개인정보 유출 신고

o (신고 주체) 개인정보를 처리하는 “개인정보처리자”, “정보통신서비스 제공자등” 그리고 개인신용정보를 처리하는 “신용정보회사등”에서의 상거래기업 및 법인이 해당합니다.

근거 법률	개인정보 보호법		신용정보법
	제34조(개인정보 유출 통지 등)	제39조의4(개인정보 유출등의 통지·신고 특례)	제39조의4(개인신용정보 누설통지 등)
신고 주체	개인정보처리자	정보통신서비스 제공자등	신용정보회사등에서의 상거래기업 및 법인에 한정

Tip	▸ 개인신용정보 누설시 통지·신고는「신용정보법」제39조의4 적용 - 신용정보회사등(상거래기업 및 법인) : “개인정보보호위원회등”에 신고 - 신용정보회사등(상거래기업 및 법인을 제외한 전체) : “금융위원회등”에 신고

o (신고 시점) 최초 개인정보의 유출 사실을 알게 되었을 때로부터의 신고 시점을 말합니다.

근거 법률	개인정보 보호법		신용정보법
	제34조	제39조의4	제39조의4
신고 시점	5일 이내	24시간 이내	5일 이내

o (신고 규모) 법에서 정하는 일정규모 이상의 정보주체에 관한 개인정보가 유출된 경우에는 신고해야 합니다.

근거 법률	개인정보 보호법		신용정보법
	제34조	제39조의4	제39조의4
신고 규모	1천명 이상	1명 이상	1만명 이상

o (신고 방법) 개인정보보호위원회 또는 한국인터넷진흥원의 홈페이지, 전화, 팩스, 이메일, 우편 등의 방법으로 신고하여야 합니다.

신고 기관명	전화번호	팩스번호	이메일	홈페이지
개인정보보호위원회 한국인터넷진흥원	118	02-405-5219	118@kisa.or.kr	개인정보보호 종합포털 (privacy.go.kr)

※ 개인정보보호 종합포털 → 민원마당 → 개인정보 유출·침해신고 → 개인정보 유출신고

o (신고 내용) 정보주체에게 해당 개인정보의 유출 사실을 통지한 결과, 유출로 인한 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 이행한 결과를 말하며 “개인정보 유출 신고서”를 제출해야 합니다.

- 유출 신고하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 신고하고, 추가로 확인되는 내용은 확인되는 즉시 신고하여야 합니다.

< 개인정보 유출 신고서 작성 방법 >

유출 신고서 양식	작성 방법
① 유출된 개인정보 항목	· 유출된 개인정보 항목을 모두 기재해야 하며, ‘등’과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 ‘전화번호’로 기재하여서는 안됨 · 유출된 개인정보의 모든 항목을 적어야 하며, 유출 규모도 현 시점에서 파악된 내용을 모두 작성
② 유출된 시점과 그 경위	· 유출시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출경위와 인지경위를 포함
③ 정보주체가 취할 수 있는 피해 최소화 조치	· 개인정보 유출로 발생 가능한 스팸 문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
④ 개인정보처리자 대응조치 및 피해 구제절차	· 유출사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재 ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등
⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	· 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재
⑥ 기타	· 유출된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재

V 정보주체 피해 구제 및 재발 방지

◇ 개인정보가 유출로 인한 정보주체 피해구제 등 지원 방안을 마련하고 유사 사고의 재발방지를 위해 대책을 수립·시행하여야 합니다.

1. 정보주체 피해 구제

o (유출여부 조회) 정보주체가 개인정보 유출여부 등을 확인가능 하도록 별도의 홈페이지 등을 제공하도록 합니다.

- 본인확인 수단으로 핸드폰, 이메일 인증 등을 활용 가능하나, 주민등록번호는 활용하지 않도록 주의합니다.

- 해당 홈페이지를 통하여 추가적인 개인정보 유출이 발생하지 않도록 웹 취약점 제거, 전송구간 암호화 등 안전조치를 이행해야 합니다.

o (민원대응) 개인정보 유출로 인한 정보주체의 피해 신고·접수, 상담·문의 등 각종 민원대응을 위한 방안을 모색해야 합니다.

- 개인정보 유출 문의에 신속히 대응할 수 있도록 상담 스크립트를 운영하고 전화, 이메일, 홈페이지, SNS 등 다양한 채널을 통해 개인정보 유출 사실, 경위 등을 확인할 수 있는 창구를 마련합니다.

- 유출 규모와 상황을 종합적으로 고려하여 원활한 민원대응을 위해 민원대응 전담부서 운영, 통신회선 증설 등이 필요할 수 있습니다.

o (현장혼잡 최소화) 유출 대응 현장에서의 긴급·돌발 상황 발생 등에 따른 혼란 최소화를 위한 방안을 강구해야 합니다.

- 현장에서 물리적 시스템 장애, 파괴 그리고 불필요한 인력 등으로 인하여 개인정보가 분실, 도난, 훼손되지 않도록 주의 하여야 합니다.

o (고객불안 해소) 보이스피싱 등 2차피해 방지를 위한 유의사항을 사전 안내하고 유출·피해 및 대응 현황 등을 실시간으로 정확하고 투명하게 공개하는 등 고객불안 해소를 위해 노력해야 합니다.

o (피해구제) 정보주체의 피해 구제 계획을 마련하고 개인정보분쟁조정위원회, 손해배상제도 등도 함께 안내하도록 합니다.

2. 재발 방지 대책 마련

o 개인정보 유출 원인, 취약점 등에 적절한 대책을 마련하고 개인정보 취급자 대상 개인정보보호 교육을 정기적으로 실시하여야 합니다.

o 개인정보 유출 대응 시나리오 작성 및 모의훈련 등을 실시하여 유출 대응 체계를 점검하고 지속적으로 보완하도록 합니다.

o 홈페이지 취약점 등으로 인한 유출 사고 예방을 위해 안전조치를 강화하도록 합니다.

- 홈페이지의 취약점을 연 1회 이상 정기적으로 점검하도록 합니다.
- 개인정보가 인터넷 상에 노출되는 것을 방지하기 위해 인증 절차 추가 및 로봇배제 규칙을 적용하여 홈페이지 접근을 제한하도록 합니다.
- 홈페이지에 첨부파일을 포함한 게시글 작성시 개인정보 포함여부를 확인하도록 합니다.
- 홈페이지 게시판 등에 정보주체가 글 작성시 개인정보가 노출되지 않도록 주의할 것을 안내하도록 합니다.
- 관리자 페이지에 접근하는 IP를 제한하거나 아이디, 비밀번호 외 추가적인 인증수단을 사용하여 접속하도록 합니다.

Tip	▸ 중소기업의 경우에는 한국인터넷진흥원에서 제공하는 웹 취약점 점검 서비스를 이용할 수 있음 – 웹 취약점 점검 신청 페이지 : KISA 보호나라 → 보안서비스 → 웹 취약점 점검

부록 1 관련 법률

1 개인정보 유출 사고 대응 계획 수립·시행

개인정보 보호법

법 제29조(안전조치의무) 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.

시행령 제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행

시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)와 그로부터 이용자(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.
1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부관리계획의 수립·시행
   가. 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항

개인정보의 안전성 확보조치 기준(고시), 시행령 제30조제1항 관련

제4조(내부 관리계획의 수립·시행) ① **개인정보처리자는** 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

개인정보의 기술적·관리적 보호조치 기준(고시), 시행령 제48조의2제1항 관련

제3조(내부관리계획의 수립·시행) ① **정보통신서비스 제공자등은** 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.

6. 개인정보의 분실·도난·누출·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다.

2 개인정보 유출 사고 대응 매뉴얼 마련

개인정보 보호법

법 제12조(개인정보 보호지침) ① 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 "표준지침"이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

표준지침 제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 **「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.**

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조회 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

3 개인정보 유출 통지 및 신고

o 개인정보처리자

개인정보 보호법

법 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.

시행령 제39조(개인정보 유출 신고의 범위 및 기관) ① 법 제34조제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 1천명 이상의 정보주체에 관한 개인정보를 말한다.

② 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 한국인터넷진흥원을 말한다.

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.

표준지침 제26조(유출 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 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 그로부터 5일 이내에 정보주체에게 알릴 수 있다.

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 피해구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실
2. 제1항의 통지항목 중 확인된 사항

③ 개인정보처리자는 개인정보 유출 사고를 인지하지 못해 유출 사고가 발생한 시점으로부터 5일 이내에 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제26조제1항 각 호의 사항을 공개할 수 있다.

제28조(개인정보 유출신고 등) ① 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 개인정보보호위원회 또는 영 제39조제2항의 전문기관에게 신고하여야 한다.

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 영 제39조제2항에 따른 전문기관의 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제26조제1항의 사항을 신고한 후, 별지 제1호서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제26조제1항에 따른 통지와 함께 인터넷 홈페이지 등에 정보주체가 알아보기 쉽도록 제26조제1항 각 호의 사항을 7일 이상 게재하여야 한다.

o 정보통신서비스 제공자등

개인정보 보호법

법 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 신고**하여야 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.

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 보급 지역으로 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.

o 신용정보회사등(상거래기업 및 법인)

신용정보법

법 제39조의4(개인신용정보 누설통지 등) ① **신용정보회사등은 개인신용정보가 업무 목적 외로 누설되었음을 알게 된 때에는 지체 없이 해당 신용정보주체에게 통지하여야 한다.** 이 경우 통지하여야 할 사항은 「개인정보 보호법」 제34조제1항 각 호의 사항을 준용한다.

② 신용정보회사등은 개인신용정보가 누설된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 신용정보회사등은 대통령령으로 정하는 규모 이상의 개인신용정보가 누설된 경우 제1항에 따른 통지 및 제2항에 따른 조치결과를 지체 없이 금융위원회 또는 대통령령으로 정하는 기관(이하 이 조에서 "금융위원회등"이라 한다)에 신고하여야 한다. 이 경우 금융위원회등은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제3항에도 불구하고 제45조의3제1항에 따른 상거래기업 및 법인은 보호위원회 또는 대통령령으로 정하는 기관(이하 이 조에서 "보호위원회등"이라 한다)에 신고하여야 한다.

⑤ 금융위원회등은 제3항에 따른 신고를 받은 때에는 이를 개인정보 보호위원회에 알려야 한다.

⑥ 금융위원회등 또는 보호위원회등은 제2항에 따라 신용정보회사등이 행한 조치에 대하여 조사할 수 있으며, 그 조치가 미흡하다고 판단되는 경우 금융위원회 또는 보호위원회는 시정을 요구할 수 있다.

⑦ 제1항에 따른 통지의 시기, 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

시행령 제34조의4(개인신용정보의 누설사실의 통지 등) ① 신용정보회사등이 법 제39조의4제1항에 따라 통지하려는 경우에는 제33조의2제3항 각 호의 어느 하나에 해당하는 방법으로 개별 신용정보주체에게 개인신용정보가 누설되었다는 사실을 통지해야 한다.

② 신용정보회사등은 법 제39조의4제3항 전단에 해당하는 경우에는 제1항에 따른 방법 외에 다음 각 호의 어느 하나에 해당하는 방법으로 금융위원회가 정하여 고시하는 기간 동안 개인신용정보가 누설되었다는 사실을 널리 알려야 한다.

1. 인터넷 홈페이지에 그 사실을 게시하는 방법
2. 사무실이나 점포 등에서 해당 신용정보주체로 하여금 그 사실을 열람하게 하는 방법

3. 주된 사무소가 있는 특별시·광역시·특별자치시·도 또는 특별자치도 이상의 지역을 보급지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷신문(「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문을 말한다)에 그 사실을 게재하는 방법

③ 제1항에도 불구하고 개인신용정보 누설에 따른 피해가 없는 것이 명백하고 법 제39조의4제2항에 따라 누설된 개인신용정보의 확산 및 추가 유출을 방지하기 위한 조치가 긴급히 필요하다고 인정되는 경우에는 해당 조치를 취한 후 지체 없이 신용정보주체에게 알릴 수 있다. 이 경우 그 조치의 내용을 함께 알려야 한다.

④ 법 제39조의4제3항 전단에서 "대통령령으로 정하는 규모 이상의 개인신용정보"란 1만명 이상의 신용정보주체에 관한 개인신용정보를 말한다.

⑤ 법 제39조의4제3항 전단에서 "대통령령으로 정하는 기관"이란 금융감독원을 말한다.

⑥ 법 제39조의4제3항 전단에 따라 신고해야 하는 신용정보회사등(상거래기업 및 법인은 제외한다)은 그 신용정보가 누설되었음을 알게 된 때 지체 없이 금융위원회가 정하여 고시하는 신고서를 금융위원회 또는 금융감독원에 제출해야 한다.

⑦ 제6항에도 불구하고 제3항 전단에 해당하는 경우에는 우선 금융위원회 또는 금융감독원에 그 개인신용정보가 누설된 사실을 알리고 추가 유출을 방지하기 위한 조치를 취한 후 지체 없이 제6항에 따른 신고서를 제출할 수 있다. 이 경우 그 조치의 내용을 함께 제출해야 한다.

⑧ 법 제39조의4제4항에서 "대통령령으로 정하는 기관"이란 「개인정보 보호법」 제34조제3항에 따른 전문기관을 말한다.

감독규정 제43조의5(신용정보 누설사실의 공시기간) 영 제34조의4제2항에 따른 "금융위원회가 정하여 고시하는 기간"이란 다음 각 호의 기간을 말한다.

1. 영 제34조의4제2항제1호의 경우: 15일
2. 영 제34조의4제2항제2호의 경우: 15일
3. 영 제34조의4제2항제3호의 경우: 7일

제43조의6(신용정보의 누설신고) 영 제34조의4제6항에 따라 신고하는 신용정보회사등은 별지 제18호 서식에 따른 신고서를 제출하여야 한다.

부록 2 유출신고서 양식

[별지 제1호서식]

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

부록 3 해킹에 의한 유출 시 조치사항

□ 해커가 삽입한 악성코드 확인 및 삭제

o 한국인터넷진흥원에서 배포중인 '휘슬'을 활용하여 웹서버에 삽입된 악성코드와 웹쉘 파일을 찾아서 삭제

※ 악성코드 탐지도구 제공 페이지 : KISA 보호나라 → 다운로드 → 휘슬 / 캐슬

□ 침해 발생 시스템의 계정, 로그 등을 점검하여 침해 현황 확인

점검 항목	점검 내용	비고
계정	· 사용하지 않는 계정 및 숨겨진 계정 확인 - 윈도우 : [관리도구]→[컴퓨터 관리]→ [로컬사용자 및 그룹]→[사용자] 정보 확인 - 리눅스 : /etc/passwd 확인	· $ 문자가 포함된 계정 확인 · 패스워드 미설정 계정 확인 · /bin/bash 설정 계정 확인
로그파일	· 이벤트 로그 및 시스템 로그 변조 유무 확인 - 윈도우 : [관리도구]→[컴퓨터 관리]→ [이벤트뷰어] 확인 - 리눅스 : /var/log/secure, message 등 확인 · 윈도우 웹로그 경로 및 변조 유무 확인 - [관리도구]→[인터넷정보서비스(IIS)관리]에서 · 리눅스 웹로그 경로 확인 - /usr/local/apache/logs 확인	· 웹로그 생성/수정 시간 확인
웹쉘	· 확장자별 웹쉘 패턴 점검 - asp, aspx, asa, cer, cdx, php, jsp, html, htm, jpg, jpeg, gif, bmp, png	· 휘슬 사용
백도어	· 네트워크 상태 확인 - nmap -sV 침해사고시스템IP · 비정상 포트 및 외부연결 확인 - 윈도우 : netstat, TCPView 등 사용 - 리눅스 : netstat -nlp, lsof -i	· 6666, 6667 등 의심 Port 확인 · 의심 Port를 사용하는 프로세스 확인
루트킷	· 숨겨진 프로세스 및 비정상 프로세스 확인 · 변조된 파일 및 시스템 명령어 확인 - Windows : IceSword, GMER 등 사용 - Linux : Rootkit Hunter, Check Rootkit 등 사용	· Rootkit Hunter 업데이트 필수

□ 로그분석 결과에 따른 접속경로 차단 등

o 로그 분석 결과 침입자 접속경로가 확인된 경우 접속경로를 차단하고 경유한 시스템은 추가적인 분석

구분	접속 경로 차단 방법	비고
서버	· 윈도우 [제어판]→[Windows 방화벽]→[일반]방화벽 사용→[예외]→원격데스크톱→편집→범위변경→사용자 지정 목록 설정(허용할IP)	특정 IP에 원격데스크톱 서비스를 허용하고 나머지 IP접속은 차단
	· 리눅스 iptables -A INPUT -p TCP --dport 22 -s 허용할IP –j ACCEPT iptables -A INPUT -p TCP --dport 22 -s –j DROP	특정 IP에 ssh 서비스를 허용하고 나머지 IP접속은 차단
네트워크	· 방화벽/라우터/스위치 access-list 101 permit tcp 허용할IP host 접근서버IP eq 22 interface ethernet 0 ip access-group 101 in	특정 IP에 ssh 서비스 허용정책을 ethernet 0 인터페이스에 인바운드 정책 적용

□ 기타 조치사항

o 서버, PC 등 정보처리시스템의 백신을 최신으로 업데이트하고 전체 디렉토리를 점검

o 직원 PC의 운영체제, 오피스 프로그램의 보안 업데이트를 실시

o 가능한 경우 침해사고 원인을 식별하고 재발방지를 위해 개인정보 유출 시스템의 휘발성 및 비활성 정보 수집

- 기술적인 사항은 한국인터넷진흥원이 배포하는 「침해사고 분석절차 안내서」 참조

※ 제공 페이지 : 한국인터넷진흥원 / 자료실 / 관련법령·기술안내서 / 기술안내 가이드 / 침해사고 분석절차 안내서

o 수사기관과 협조하여 유출된 개인정보를 회수하기 위한 조치를 강구

부록 4 경찰 수사 및 침해사고 신고

1 경찰 수사

o 해커 등 개인정보 유출자 검거 및 개인정보 회수를 위한 조치가 필요한 경우에는 경찰청 사이버 안전국에 범인 검거를 위한 수사를 요청하고 유출된 개인정보 회수를 위한 조치를 실시

※ 사이버범죄 신고 : 경찰청 → 신고/지원 → 사이버범죄 신고/상담

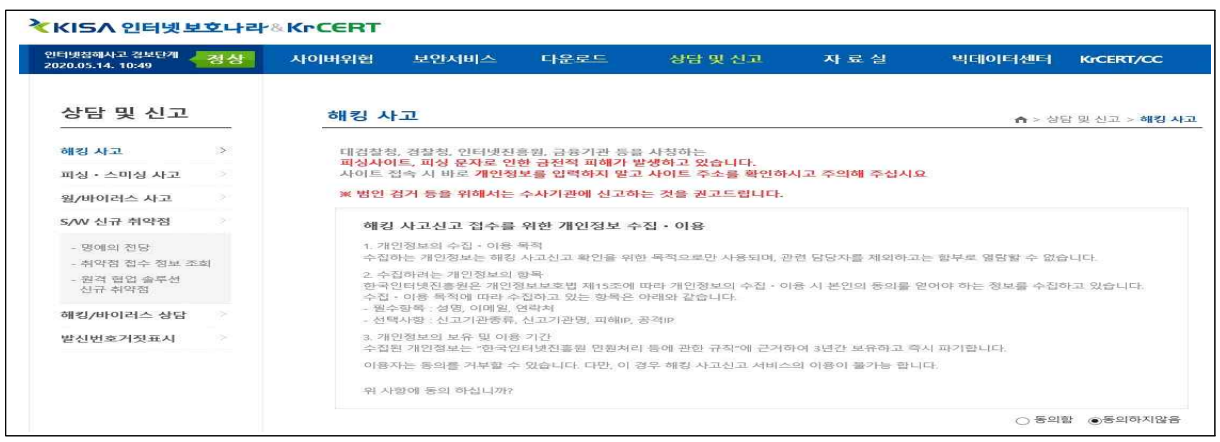
2 침해사고 신고

o 해킹 등 침해사고가 발생하면 즉시 관계 기관에 신고하여 사고 원인분석 및 취약점 보완조치 등을 실시

- 공공부문 : 국가정보원

- 민간부문 : 과학기술정보통신부 또는 한국인터넷진흥원

※ 침해사고 신고 : KISA 보호나라 → 상담 및 신고 → 해킹 사고, ☏ 국번없이 118



부록 5 개인정보 유출에 따른 2차 피해 유형 및 대응방안

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	정보주체 대응 방안
금전적	온라인 사기쇼핑	주민등록번호, 카드번호, 유효기간 등	① 카드번호, 유효기간으로 온라인 결제가 가능한 국내외 홈쇼핑 사이트에 접속 ② 홈쇼핑 홈페이지, ARS를 통한 온라인 사기 결제·주문	• 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국소비자원 소비자 상담센터(☏1372) 등
	명의도용을 통한 통신서비스 가입	이름, 주소, 주민등록번호 등	① 유출된 개인정보를 이용하여 휴대전화, 인터넷전화 등 가입 ※ 통신서비스 가입 시 본인확인절차가 있으므로 주민등록증 위조 등 추가적인 불법 행위 수반이 예상됨 ② 불법 가입한 전화번호로 스팸을 발송하여 금전적 이익을 취득함 ※ 명의를 도용당한 사람은 서비스 이용제한을 당하거나 명의도용 소명절차를 밟는 등 피해를 당함	• 한국정보통신진흥협회(KAIT)의 명의도용방지서비스(M-Safer)를 통한 불법 통신서비스 신규가입 여부 확인 ※ 신고기관 : 통신민원조정센터(msafer.or.kr) ※ 명의도용방지서비스(M-Safer) : 통신서비스 신규가입시 이메일·문자로 가입여부 통보
	명의도용을 통한 신용카드 복제	이름, 신용카드 번호, 유효기간 등	① 유출된 개인정보를 이용하여 신용카드 불법 복제 ※ 특수장비를 이용하여 카드번호, 유효기간, 이름 등으로 복제 가능 ② 불법 복제된 카드를 국내외에서 활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능	• 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☏1332)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	정보주체 대응 방안
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취	• 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	① 경찰, 금융감독당국 또는 금융회사 직원을 사칭하여 전화 ② 금융관련 업무 목적 사칭을 통한 개인정보·금융정보 탈취(비밀번호, 보안카드번호 등) ③ 유출된 금융사를 사칭, 개인정보 유출 확인을 빙자하여 ARS를 통해 계좌번호/비밀번호 등 금융정보 입력 요청	• 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름, 이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118) ※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	정보주체 대응 방안
	휴대전화/이메일 스팸발송	휴대전화 번호, 이메일 주소 등	① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송 ※ 유출된 모든 휴대전화, 이메일로 도박 등 스팸 무작위 발송 가능 ※ 신용정보, 연소득등 활용 대출 스팸 발송, 자동차 보유여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능 ② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신	• 지능형 스팸차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118) ※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스
	사회공학적 기법을 활용한 악성코드 유포메일 발송	이메일주소 등	① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송 ② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭 ③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄	• 의심가는 이메일을 받은 경우 함부로 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸대응센터(☏118)