발 간 등 록 번 호
11-1790365-100051-14

OPEN 출처표시
공공누리 공공저작물 자유이용허락

개인정보 유출등 대응 안내서

2026. 9.

개인정보보호위원회
Personal Information Protection Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

발 간 등 록 번 호
11-1790365-100051-14

개인정보 유출등 대응 안내서

2026. 9.

개인정보보호위원회
Personal Information Protection Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

개인정보 유출등 대응 안내서

안내 사항

발간 목적

본 안내서는 개인정보의 유출등이 발생한 경우, 이에 대한 신속한 대응 및 조치를 통한 피해 확산 방지와 정보주체에 대한 피해구제를 위한 사항을 안내하기 위한 목적으로 마련되었습니다.
개인정보처리자는 처리하는 개인정보의 흐름, 처리하는 방법 및 환경, 개인정보의 유형 등에 따라 자체 환경을 고려하여 개인정보 유출등 사고 대응 계획을 수립·시행하여야 합니다.

제·개정 이력

개인정보보호 관련 법·제도 및 환경 변화를 반영하여 다음과 같이 개정하였습니다.

일자	주요 내용
'16. 8. 발간	「정보통신서비스 제공자등을 위한 개인정보 유출 대응 매뉴얼」 발간(방통위)
'20. 12. 개정	「개인정보 보호법」 개정('20년) 사항 반영 및 소관 부처 변경(방통위→개인정보위)
'23. 9. 개정	개인정보 유출 등 사고에 신속한 대응을 위한 최소한의 사항 안내
'24. 3. 개정	「개인정보 보호법」 개정('24.3.15. 시행) 사항 반영
'26. 9. 개정	「개인정보 보호법」 개정('26.9.11. 시행) 사항 반영

재검토 기한

안내서의 최신성을 유지하기 위해 발간일(2026년 9월)을 기준으로 3년마다(매 3년째의 12.31.까지를 말함) 보완 및 개선 등의 조치를 취할 예정입니다.

저작권 표시

본 안내서 내용의 무단전재를 금하며, 가공·인용할 때는 출처를 밝혀 주시기 바랍니다.

* 출처 : 개인정보보호위원회 「개인정보 유출등 대응 안내서」 2026.9.

문의처

안내서 내용 관련 문의는 다음의 연락처로 주시기 바랍니다.
- 개인정보보호위원회 조사총괄과(☎02-2100-3102)
- 한국인터넷진흥원 사이버민원·상담센터(국번 없이 ☎118)

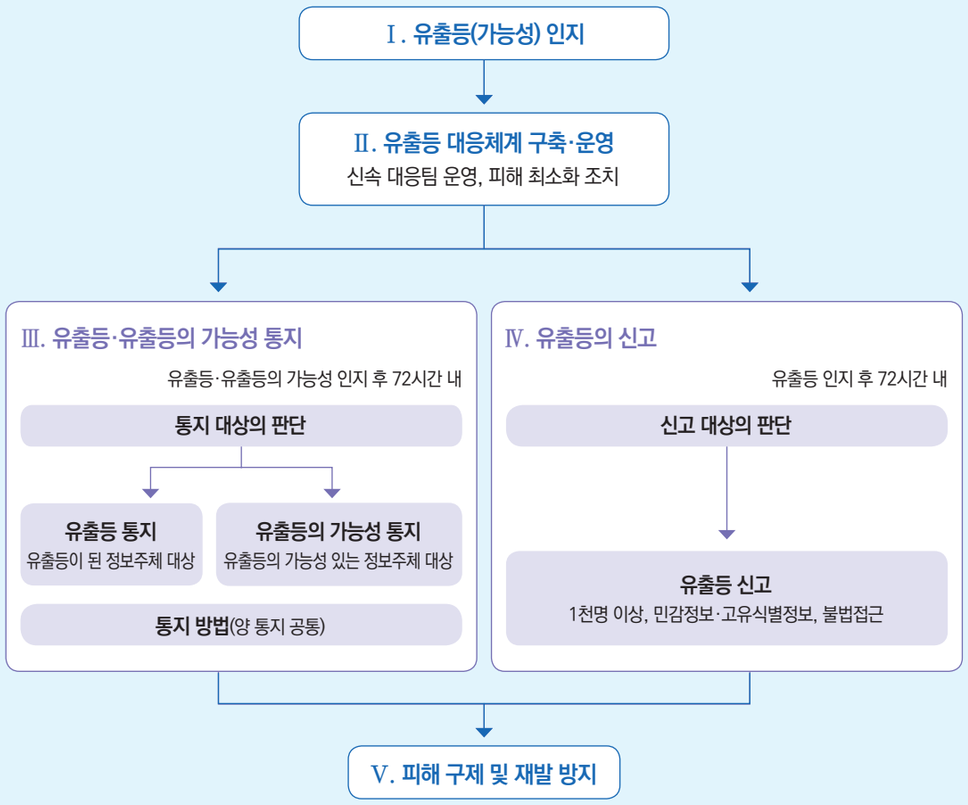
관계법령

「개인정보 보호법」 제34조 및 동법 시행령 제39조~제40조 등

※ 법령 최신 자료는 국가법령정보센터(www.law.go.kr), 개인정보 보호 안내서 최신 자료는 개인정보보호위원회 누리집*, 개인정보 포털**을 참고
* 개인정보보호위원회 누리집(www.pipc.go.kr) : 법령 〉 법령정보 〉 안내서
** 개인정보 포털(www.privacy.go.kr) : 자료 〉 자료보기 〉 안내서

한눈에 보는 유출등 대응 안내서

개인정보 유출등 대응 흐름



유출등·유출등의 가능성 통지·신고 방법

① 유출등 통지

요건

유출등이 된 사실을 알게 된 경우
(정보주체 1명 이상)

대상·기한

정보주체에게 개별 통지
유출등 인지 후 72시간 내
지연 사유 : 유출등 방지를 위한 긴급 조치 / 천재지변 등

통지 사항

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 정보주체가 할 수 있는 피해 최소화 조치
4. 개인정보처리자 대응조치 및 피해 구제절차
5. 피해가 발생한 경우 신고·상담 부서 및 연락처
6. 정보주체의 법적 권리와 그 행사 방법

통지 방법

서면·전자우편·팩스·전화·문자 등 개별 통지
연락처를 알 수 없는 등 정당한 사유 시
홈페이지 30일 이상 게시

② 유출등의 가능성 통지

요건(어느 하나 해당)

① 불법적인 접근이 발생하여 유출등 정황이 있으나 정보주체 특정 곤란
② 불법 거래 등 일부 유출등 확인으로 타 정보주체의 유출등의 가능성 인정

대상·기한

유출등의 가능성 있는 정보주체에게 개별 통지
유출등의 가능성 인지 후 72시간 내
지연 사유 : 천재지변 등에 한정

통지 사항

1. 유출등의 가능성이 있는 개인정보의 항목
2. 유출등이 있었을 것으로 의심 또는 인정되는 시점과 그 경위
3. 정보주체가 할 수 있는 피해 최소화 조치
4. 개인정보처리자 대응 조치 및 피해 구제절차
5. 피해가 발생한 경우 신고·상담 부서 및 연락처
6. 유출등 확정 시 추가 통지를 하겠다는 사실

※ 법적 권리·피해 구제 정보는 미포함

통지 방법

유출등 통지와 동일
유출등 확정 시 인지 후 72시간 내 유출등 통지 또는 유출등이 없었던 사실 통지

③ 유출등 신고

요건(어느 하나 해당)

① 1천 명 이상 유출등이 된 경우
② 민감정보·고유식별정보가 유출등이 된 경우
③ 외부로부터의 불법적인 접근에 의해 유출등이 된 경우

기관·기한

개인정보보호위원회에 신고
유출등 인지 후 72시간 내
지연 사유 : 천재지변 등에 한정

신고 사항

유출등 통지의 통지 사항과 동일

[우선 신고·추가 신고]

구체적 내용을 확인하지 못한 경우
확인된 내용을 우선 신고한 후,
추가 확인 시 추가 신고임을 명시하여 신고

신고 방법

개인정보 유출신고 시스템 brss.pipc.go.kr

※ 개인정보의 회수·삭제로 권익 침해 가능성이 현저히 낮아진 경우 신고하지 않을 수 있음

용어정의

① 개인정보·개인정보처리자

개인정보(법 제2조제1호)

살아 있는 개인에 관한 정보로서 다음의 어느 하나에 해당하는 정보

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

다. 가명처리함으로써 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(가명정보)

개인정보처리자(법 제2조제5호)

업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관·법인·단체 및 개인 등

② 유출등

분실·도난·유출

법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태

위조

권한 없는 자가 개인정보를 새롭게 생성하는 것

변조

권한 없이 기존 개인정보에 변경을 가하는 것

훼손

개인정보를 못쓰게 만드는 것,
즉 효용을 해하는 것

③ 민감정보·고유식별정보

고유식별정보(법 제24조제1항, 영 제19조)

법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보

1. 주민등록번호 (주민등록법 제7조의2제1항)
2. 여권번호(여권법 제7조제1항제1호)
3. 운전면허의 면허번호 (도로교통법 제80조)
4. 외국인등록번호 (출입국관리법 제31조제5항)

민감정보(법 제23조제1항, 영 제18조)

사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 사생활을 현저히 침해할 우려가 있는 개인정보로서 다음의 정보

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 범죄경력자료 (형의 실효 등에 관한 법률 제2조제5호)
3. 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 신체적·생리적·행동적특징 정보
4. 인종이나 민족에 관한 정보

C O N T E N T S

용어의 정의 ····· 7

Ⅰ 개요 9
1. 필요성 ····· 10
2. 적용 범위 ····· 11
3. 법적 의무사항 ····· 12
4. 적용 대상 ····· 17

Ⅱ 개인정보 유출등 대응체계 구축·운영 21
1. 유출등 사고 발생 보고 및 신속 대응팀 구성·운영 ····· 22
2. 피해 최소화 및 긴급 조치 ····· 25

Ⅲ 개인정보 유출등·유출등의 가능성 통지 31
1. 개인정보 유출등의 통지 ····· 32
2. 개인정보 유출등의 가능성 통지 ····· 38

Ⅳ 개인정보 유출등의 신고 43

Ⅴ 정보주체 피해 구제 및 재발 방지 55
1. 정보주체의 피해 구제 ····· 56
2. 재발 방지 대책 마련 ····· 63

부록 65

용어의 정의

1. "**개인정보**"란 살아 있는 개인에 관한 정보로서 다음의 어느 하나에 해당하는 정보를 말한다.
   - 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
   - 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보 이 경우 쉽게 결합할 수 있는지의 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 함
   - 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(가명정보)
2. "**개인신용정보**"란 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 다음의 어느 하나에 해당하는 정보를 말한다.
   - 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보
   - 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보
3. "**개인정보처리자**"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "**신용정보회사등**"이란 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 신용정보제공·이용자를 말한다.

   ※ 세부 정의는 「신용정보의 이용 및 보호에 관한 법률」 제2조(정의)를 참조
5. "**상거래기업 및 법인**"이란 금융위원회의 감독을 받지 아니하는 신용정보제공·이용자를 말한다.

Ⅰ

개요

Ⅰ 개요

1 필요성

- 개인정보처리자가 처리하는 개인정보에 분실·도난·유출·위조·변조 또는 훼손(이하 “유출등”)이 발생한 경우, 신속한 대응과 조치를 통한 피해 확산 방지 및 정보주체에 대한 피해구제 방법 안내의 중요성이 증대되고 있다.

- 따라서 본 안내서는 개인정보 유출등과 관련하여 신속한 대응과 피해 최소화를 위해 필요한 최소한의 사항을 안내한다.
  - 특히, 2026년 9월 시행되는 개정 「개인정보 보호법」 제34조(개인정보 유출등의 통지·신고)와 「신용정보의 이용 및 보호에 관한 법률」(이하 「신용정보법」이라 한다) 제39조의4(개인신용정보 누설통지 등)에 대한 내용도 포함한다.
    ※ 「신용정보법」 제39조의4(개인신용정보 누설통지 등)에서 개인신용정보가 신용정보회사등의 업무 목적 외로 누설된 경우도 포함한다.

- 개인정보처리자 및 신용정보회사등이 처리하는 개인(신용)정보의 종류, 처리하는 방법 및 환경, 개인정보처리주체의 유형(성격) 등에 따라 다르게 적용될 수 있으므로 각각의 환경을 고려하여 개인정보 유출등 사고 대응 매뉴얼 마련이 필요하다.

2 적용 범위

- 개인정보처리자가 처리하는 개인정보에 유출등이 발생한 경우에는 「개인정보 보호법」 제34조가 적용되어 유출등 통지 및 유출등 신고의 대상이 된다.
- 다만, 신용정보회사등의 개인신용정보가 누설된 경우에는 「신용정보법」 제39조의4가 우선 적용된다.

※ 신용정보회사등의 개인신용정보 누설 통지·신고 의무에 대하여는 부록 1 「신용정보회사등의 개인신용정보 누설 통지·신고」 참고한다.

3 법적 의무사항

■ 개인정보 유출등 사고 대응 계획 수립·시행

- 개인정보 유출등 사고 대응 계획에 관한 사항을 내부 관리계획에 포함하여 수립·시행하여야 한다.

개인정보 보호법

제29조(안전조치의무) 개인정보처리자는 개인정보가 유출등이 되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

개인정보 보호법 시행령

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검
가. 법 제28조제1항에 따른 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항
다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항

개인정보의 안전성 확보조치 기준

제4조(내부 관리계획의 수립·시행 및 점검) 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. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

14. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

■ 개인정보 유출등 대응 매뉴얼 마련

- 개인정보 유출등 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 공공기관 및 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자는 “개인정보 유출등 사고 대응 안내서”를 마련할 것을 권고한다.

개인정보 보호법

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.

표준 개인정보 보호지침

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

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

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

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

개인정보 유출등의 통지·신고

- 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 해당 정보주체에게 유출등 사실을 통지하여야 한다.
- 개인정보의 유형, 정보주체에게 미치는 영향 및 유출등의 위험 정도를 고려할 때 유출등의 가능성이 있음을 알게 된 경우에는 72시간 이내에 유출등의 가능성이 있는 모든 정보주체에게 그 사실을 통지하여야 한다.
- 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우, 민감정보 또는 고유식별정보가 유출등이 된 경우, 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우에는 72시간 이내에 개인정보보호위원회에 신고하여야 한다.

개인정보 보호법

제34조(개인정보 유출등의 통지·신고) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
6. 개인정보 유출등으로 인한 제39조에 따른 손해배상과 제39조의2에 따른 법정손해배상의 청구 및 제43조에 따른 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보
7. 그 밖에 개인정보가 유출등이 된 정보주체의 보호를 위하여 대통령령으로 정하는 사항

② 제1항에도 불구하고 개인정보의 유형, 정보주체에게 미치는 영향 및 유출등의 위험 정도를 고려하여 대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때에는 지체 없이 유출등의 가능성이 있는 모든 정보주체에게 피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항을 알려야 한다.

③ 개인정보처리자는 개인정보가 유출등이 된 경우에는 해당 개인정보의 회수·삭제 등 피해 확산을 방지하기 위한 조치를 포함하여 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

④ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 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.

⑤ 제1항·제2항에 따른 통지 및 제4항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다

개인정보 보호법 시행령

제39조(개인정보 유출등의 통지) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 즉시 정보주체에게 알릴 수 있다.

1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

② 제1항에도 불구하고 개인정보처리자는 같은 항에 따른 통지를 하려는 경우로서 법 제34조제1항

제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그 때까지 확인된 내용 및 같은 항 제3호부터 제6호까지의 사항을 서면등의 방법으로 우선 통지해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지해야 한다.

③ 제1항 및 제2항에도 불구하고 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다

제39조의2(개인정보 유출등의 가능성 통지 대상) ① 법 제34조제2항에서 "대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때"란 다음 각 호의 구분에 따른 때를 말한다.

1. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 불법적인 접근이 발생하여 개인정보 유출등이 의심되는 정황이 있으나 그 개인정보의 정보주체를 특정하기 곤란한 경우 : 해당 불법적인 접근을 알게 된 때
2. 개인정보처리자가 처리하는 개인정보가 법, 이 영 또는 개인정보 보호에 관한 다른 법령을 위반하여 제3자에 의해 거래되는 등 일부 개인정보가 유출등이 된 사실이 확인된 경우로서 다른 정보주체에 관한 개인정보도 유출등이 되었을 수 있다고 인정되는 경우 : 해당 사실을 알게 된 때

② 법 제34조제2항에서 "피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 유출등의 가능성이 있는 개인정보의 항목
2. 유출등이 있었을 것으로 의심 또는 인정되는 시점과 그 경위
3. 법 제34조제1항제3호부터 제5호까지의 사항
4. 유출등의 여부가 확정될 경우의 추가 통지를 하겠다는 사실

제39조의3(개인정보 유출등의 가능성 통지 시기 · 방법 등) ① 개인정보처리자는 법 제34조제2항에 따라 제39조의2제2항 각 호의 사항을 통지하려는 경우 같은 조 제1항 각 호의 구분에 따른 때부터 72시간 이내에 서면등의 방법으로 해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 기한 내에 통지하기 곤란한 경우에는 해당 사유가 해소된 후 즉시 정보주체에게 통지해야 한다.

② 개인정보처리자는 제1항에 따른 기한 내에 개인정보가 실제로 유출등이 된 사실을 확인한 경우에는 법 제34조제2항에 따른 통지에 갈음하여 같은 조 제1항에 따른 통지를 해야 한다.

③ 법 제34조제2항에 따른 통지를 한 개인정보처리자는 개인정보가 실제로 유출등이 되지 않은 사실을 확인한 경우 즉시 정보주체에게 그 사실을 통지해야 한다.

④ 개인정보처리자는 법 제34조제2항 또는 이 조 제3항에 따른 통지의 대상인 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 개인정보 유출등의 가능성(제39조의2제2항 각 호의 사항을 포함한다) 또는 개인정보가 실제로 유출등이 되지 않은 사실을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 법 제34조제2항 및 이 조 제3항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 않는 개인정보처리자의 경우에는 사업장

등의 보기 쉬운 장소에 30일 이상 게시하는 것으로 법 제34조제2항 및 이 조 제3항의 통지를 갈음할 수 있다.

제40조(개인정보 유출등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제4항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 즉시 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보 또는 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제1항에도 불구하고 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항 1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제6호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

③ 법 제34조제4항 전단 및 후단에서 “대통령령으로 정하는 전문기관”이란 각각 한국인터넷진흥원을 말한다.

4 적용 대상

■ 개인정보의 분실·도난·유출

- 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태를 말한다.(표준 개인정보 보호지침 제25조 참조)

FAQ 질의 응답

Q1 개인정보가 외부에 노출되었는데, 개인정보 유출에 해당하나요?

답변 제3자가 개인정보의 내용을 취득하여야만 유출되었다고 보는 것은 아니며, 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 되었다면 개인정보의 유출로 봅니다.

다만 단순히 접근이 가능한 상태에 놓였다는 사실만으로는 부족하고, 제3자가 실제로 접근하거나 열람할 수 있었는지 등을 종합하여 구체적인 사실관계에 따라 판단합니다.

사례 1 개인정보 유출로 판단하지 않은 경우

법원은 개인정보의 유출을 "개인정보가 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이른 것"으로 정의하면서, 개인정보가 여전히 처리자의 관리·통제 아래에 있고 제3자에게 실제로 열람되거나 접근되지 않은 상태라면, 기술적·관리적 보호조치가 미흡하여 외부에서 접근할 수 있는 상태에 놓여 있었다는 사정만으로 곧바로 유출이 있었다고 볼 수는 없다고 판단한 바 있습니다. 해당 사안은 시스템 연동 점검을 위해 임시로 부여받은 계정정보를 점검 종료 후에도 삭제하지 않아 외부 사이트와 서버가 계속 연동된 상태로 남아 있었으나, 그 경로를 통해 이용자의 개인정보가 제3자에게 실제 열람되거나 접근되지 아니한 상태라면, 정보통신서비스 제공자의 기술적·관리적 보호조치에 미흡한 점이 있어서 제3자가 인터넷상 특정 사이트를 통해 정보통신서비스 제공자가 보관하고 있는 개인정보에 접근할 수 있는 상태에 놓여 있었다고 하더라도 그것만으로 바로 개인정보가 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 내용을 알 수 있는 상태에 이르게 되었다고 할 수는 없다고 판시하였습니다.

(대법원 2014. 5. 16. 선고 2011다24555 판결)

사례 2 개인정보 유출로 판단한 경우

개인정보가 포함된 문서가 공개 설정 오류로 외부에 게시되어 불특정인이 해당 게시물에 접속하여 첨부파일을 내려받았다면, 개인정보처리자가 그 사실을 인지한 후 즉시 비공개 조치를 하였더라도 공개된 기간 중 한 차례라도 다운로드가 이루어진 이상 개인정보가 유출된 것으로 봅니다.

총 7회의 다운로드 중 업무 담당자와 민원 당사자의 접근을 제외하면 제3자로 추정되는 접근이 2회에 불과하고, 시스템상 해당 첨부파일에 접근한 IP를 특정할 수 없어 제3자 여부를 확인할 수 없다 하더라도, 이는 유출을 부정할 근거가 되지 못하므로 이를 이유로 개인정보의 유출로 보지 않는 것은 타당하지 않습니다.

개인정보의 위조·변조·훼손

- 개인정보의 위조는 권한 없는 자가 개인정보를 새롭게 생성하는 것을 말하며, 개인정보의 변조는 권한 없이 기존 개인정보에 변경을 가하는 일을 의미한다.
- 개인정보의 훼손이란 개인정보를 못 쓰게 만드는 것, 즉 효용을 해하는 것을 의미한다. 개인정보 훼손으로 판단하기 위해서는 손실이 발생하여야 한다.

※ 훼손으로 판단하는 개인정보 손실의 기준은 「개인정보의 안전성 확보조치 기준」 제4조(내부 관리 계획의 수립·시행 및 점검) 등을 참고하여 개인정보처리자의 상황에 따라 달리 판단될 수 있다.

FAQ 질의 응답

Q1 개인정보 훼손의 예를 알려주세요

답변 훼손이란 개인정보를 못 쓰게 만드는 것, 즉 개인정보의 효용을 해하는 것을 의미하며, 다음과 같은 경우를 예로 들 수 있습니다.

- 데이터가 실수로 또는 권한 없는 사람에 의해 삭제된 경우
- 암호화된 데이터의 복호화 키를 분실한 경우
- 백업 등을 통해서도 개인정보를 복원할 수 없는 경우

Q2 랜섬웨어 감염으로 개인정보가 암호화된 경우, 개인정보 훼손에 해당하나요?

답변 복구가 불가능한 경우에는 개인정보 훼손에 해당할 수 있으며, 복구 가능 여부에 따라 다음과 같이 구분됩니다.

사례 1 훼손으로 판단한 경우

쇼핑몰 회원 약 900명의 개인정보가 랜섬웨어에 의해 암호화되어 복호화가 불가능한 상태가 되었고, 별도 백업이 없어 홈페이지를 신규 구축하고 회원가입을 다시 받아야 했던 경우

사례 2 훼손으로 판단하지 않은 경우

ERP 서버 드라이브 전체가 랜섬웨어에 감염되어 임직원 및 거래처 직원 1,900여 명의 개인정보가 암호화되었으나, 사고 인지 즉시 그룹 백업시스템을 통해 사고 인지 후 5시간, 사고 발생 후 24시간 내에 데이터와 시스템을 복구한 경우

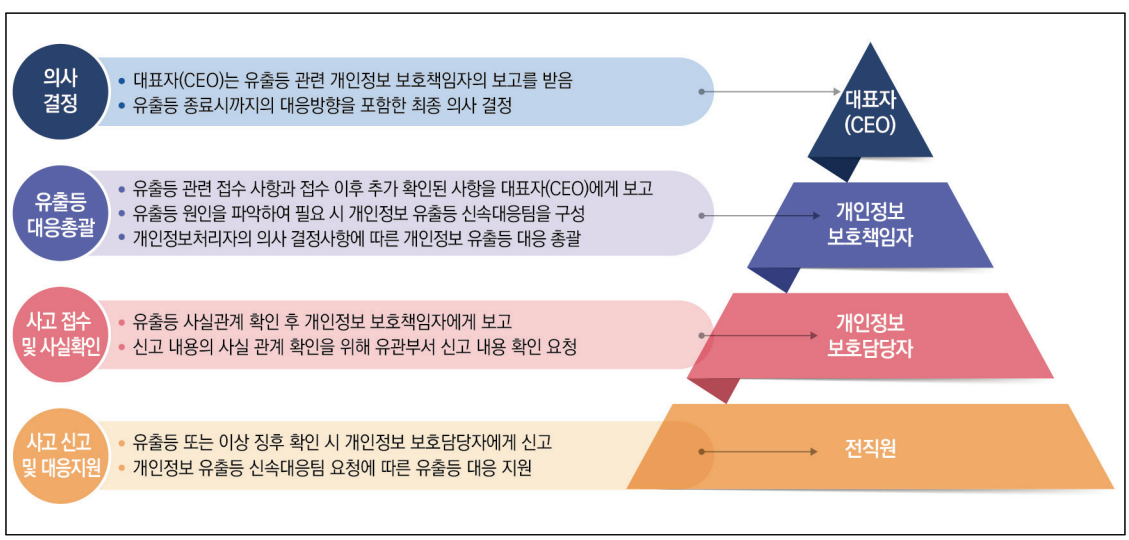
Ⅱ

개인정보 유출등 대응체계 구축·운영

Ⅱ 개인정보 유출등 대응체계 구축·운영

1 유출등 사고 발생 보고 및 신속 대응팀 구성·운영

- 개인정보의 유출등 사실을 알게 된 경우, 개인정보 보호책임자는 즉시 대표자(CEO)에게 보고하고 개인정보 보호·정보보호 부서 등을 중심으로 개인정보 유출등 신속대응팀을 구성하여 피해확산 방지 및 최소화를 위한 조치를 하여야 한다.



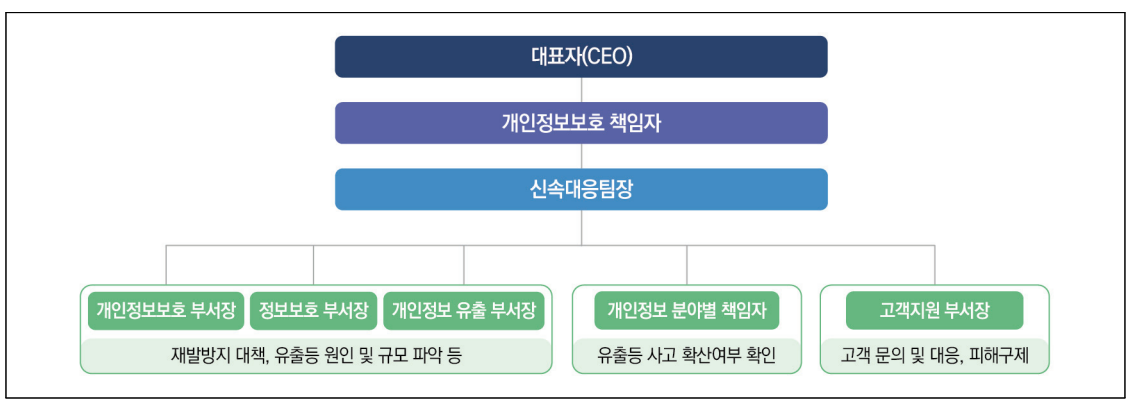
개인정보 유출등 대응체계(예시)

개인정보 유출등 사고 발생 사실 보고 체계

- 전직원
  - 개인정보 유출등 사실을 발견하거나 의심스러운 정황을 알게 된 경우에는 즉시 개인정보 보호담당자에게 전화, 이메일 등으로 신고해야 한다.
- 개인정보 보호담당자
  - 신고를 받은 즉시 관련자에게 유출등 규모, 경로 등 유출등 사실 여부를 확인 요청하고, 개인정보 보호책임자에게 유출등 사실 및 피해 규모, 대응 상황 등을 신속하게 보고해야 한다.
- 개인정보 보호책임자
  - 해당 시점까지 파악된 현황을 대표자(CEO)에게 신속하게 보고하고 새로운 상황이 발생할 때마다 수시로 보고해야 하며, 개인정보 유출등이 확인되는 즉시 '개인정보 유출등 신속대응팀(TF)'을 구성·운영하여야 한다.
- 대표자(CEO)
  - '개인정보 유출등 신속대응팀'을 중심으로 유관부서가 유기적으로 대응하도록 지원하고 유출등 대응에 대한 방향성 제시 등 의사결정을 진행한다.

개인정보 유출등 신속대응팀 구성 및 운영

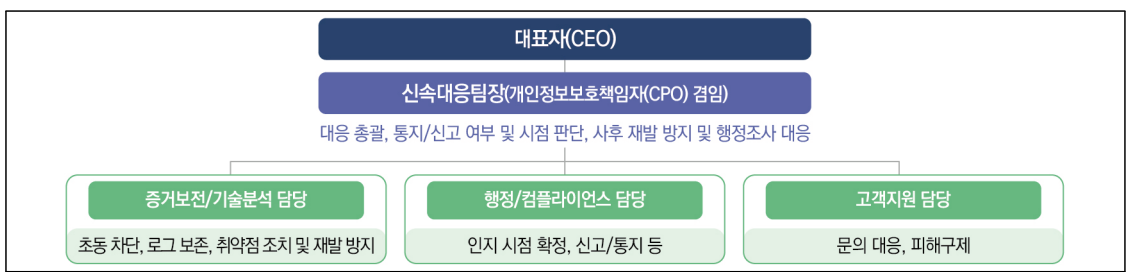
- 개인정보보호책임자는 개인정보 보호·정보보호 부서 등을 중심으로 개인정보 유출등 신속대응팀을 구성하여 사고 분석, 피해 확산 방지 및 최소화, 사고 복구 및 예방 조치 등을 하여야 한다.
- 아래는 중견기업 이상 기준 조직 구성 예시로 개인정보 유출등 신속대응팀은 개인정보보호책임자(CPO)를 중심으로 개인정보보호·정보보호·법무·고객지원 부서 등 관련 인력으로 구성하며, 내부 조직 및 인력을 효율적으로 분배하여 유출등 원인 분석 및 긴급 대응, 피해 최소화 조치, 관계기관 신고·정보주체 통지, 이용자 피해구제, 고객지원 등 업무를 세분화하여 신속히 대응한다.



중견기업 이상 규모의 개인정보 유출등 신속대응팀 역할(예시)

부서	주요 역할
개인정보보호 부서	유출등 인지·보고, 신속대응팀 총괄 운영, 유출등 신고, 유출등 규모 파악, 정보주체 유출등 통지, 재발 방지 조치 결과 전직원 교육·전파
정보보호 부서	증거 보전 및 포렌식, 유출등 원인 분석 및 경로 파악, 시스템 접근 차단 등 긴급 기술조치, 다크웹 등 유출등 정보 유통 모니터링 및 삭제 요청, 재발 방지를 위한 보안 조치
개인정보 유출 부서장	유출등 발생 사실 즉시 보고, 해당 부서 인력·자료 협조, 재발 방지 대책 수립 지원
개인정보 분야별 책임자	관리 시스템에서 개인정보 유출등 확산여부, 악성코드 감염 여부 등 확인
고객지원 부서	정보주체 대상 피해구제 접수·처리, 고객 문의 및 민원 대응, 피해신고 창구 운영, 고객 불안 해소 조치
법무 부서	법적 의무사항 검토, 수사기관 협조 및 대응, 손해배상 등 법적 분쟁 대응, 외부 법률 자문 연계
홍보 부서	유출등 관련 공식 입장문 작성·배포, 언론 보도 모니터링 및 대응, 대외 공지 채널 관리, 루머·오보 확산 방지 조치
대관 부서	관계 행정기관·감독기관 대응 및 협력, 국회·언론 등 외부 기관 커뮤니케이션, 행정처분 관련 의견 제출 및 소명 지원

● 아래는 비교적 규모가 작은 중소기업 환경을 고려한 조직 구성 예시이다.



중소기업 이하 규모의 개인정보 유출등 신속대응팀 역할(예시)

담당	주요 역할 예시
신속대응팀장	[대응 총괄 및 최종 의사결정] • 상황 통제 및 부서별 임무 부여 • 통지·신고 대상 여부, 통지 시점(유출등 가능성 단계 포함)에 대한 판단 및 승인 [사후 관리 및 행정조사 총괄 대응] • 유출등 종결 후 재발 방지 대책 기획 및 이행 점검 • 개인정보보호위원회(PIPC) 현장 행정조사 대응
증거보전/ 기술분석 담당	[포렌식 증거 및 원본 보전] • (가상서버) 접속 차단 전 스냅샷 및 가상디스크 보존 • (물리/PC) 네트워크 분리(랜선 제거) 후 디스크 보관 • 유출등 시점 전후 접속기록·보안 로그 일체 우선 백업 [피해 최소화 및 원인 파악] • 증거 보전 완료 후 시스템 접근 차단 및 취약점 조치 • 유출등의 경로, 항목, 규모(정보주체 수) 등 분석 • 위조·변조·훼손 여부 및 데이터 무결성 확인

담당	주요 역할 예시
행정/ 컴플라이언스 담당	[인지 시점 확정 및 기록 관리] • 최초로 유출등 또는 유출등 가능성을 인지한 시점 기록 • 대응 전 과정을 기록 및 보존 [관계기관 신고] • 개인정보 보호법 : 법령상 신고요건에 해당하는 경우 인지 후 72시간 내 개인정보보호위원회 또는 한국인터넷진흥원에 신고 [정보주체 유출등 통지] • 인지 후 72시간 내 개별 통지 발송(이메일, 문자 등) • 홈페이지 팝업 공지 게재(법정 필수 항목 포함 확인)
고객지원 담당	[고객 응대 및 2차 피해 구제] • 전용 CS 창구 개설 및 고객 문의 응대 매뉴얼(Q&A) 숙지 • 스미싱, 보이스피싱 등 2차 피해 구제 절차(분쟁조정) 안내

2 피해 최소화 및 긴급 조치

■ 긴급 차단 조치

- 추가 유출등 및 피해확산을 방지하기 위해 유출등과 관련된 시스템·계정·접근 경로를 즉시 차단한다.
  - 유출등이 된 시스템에 대한 외부 접속 차단 및 격리 조치를 시행한다.
  - 유출등에 사용된 것으로 의심되는 계정, 인증 정보(인증키, API 키, 토큰, 인증서 등)의 권한을 정지하고 비밀번호 등을 변경한다. 관리자 계정, 서비스 계정, 클라우드 액세스 키(Access Key)를 포함하여 점검한다.

    ※ 일방향 암호화되지 않은 비밀번호가 유출되었거나, 해커 등이 이용자의 비밀번호를 알고 있다고 판단되는 경우에는 개인정보취급자 및 이용자가 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해를 방지한다.
  - 유출등에 사용된 활성 세션이 있는 경우 즉시 강제 종료한다. 세션 토큰, 쿠키 기반 인증을 사용하는 경우 서버 측 세션 무효화 및 토큰 폐기(서명키 교체 포함)을 병행한다.
  - 취약점이 확인된 부분에 대해서는 즉시 보완 조치(보안패치, 설정 변경, 웹쉘 삭제 등)를 적용하되, 조치 전 해당 상태를 증거로 보존(스크린샷, 파일 원본 백업 등)한 후 조치한다.
- 영향받는 시스템이 클라우드, 호스팅 환경에 위탁하여 운영하는 경우, 자체 조치와 더불어 즉시 해당 서비스 제공업체(CSP, MSP) 기술지원 센터에 연락하여 긴급 방화벽 차단, 스냅샷 생성 등에 대한 기술지원을 요청한다.

유출등 범위 확인 및 증거 보존

- 유출등이 된 개인정보의 항목·규모·경위를 파악하고, 사후 원인분석 및 행정조사 대비를 위해 관련 증거를 보전한다.
  - 시스템 접속기록, 네트워크 로그, 보안장비 로그 등 관련 증거를 변조 불가능한 형태로 보존한다.
  - 침해 시스템의 디스크 이미지를 백업하여 포렌식 분석에 활용할 수 있도록 한다.
  - 영향받는 시스템이 가상서버, 클라우드 환경인 경우, 원본 상태의 스냅샷(Snapshot)을 생성하여 보존한다.
  - 로그의 자동 삭제·보존기간 만료로 인한 소실을 방지하기 위해, 유출등 인지 즉시 관련 로그의 자동 삭제 설정을 중지하거나 별도 저장소로 복사·보존한다.
  - 영향 범위(피해 정보주체 수, 유출등이 된 항목 등)는 우선 확인된 내용을 기준으로 정리하고, 추가 확인 사항은 즉시 갱신한다.
- 초동 대응 및 원인 분석을 위해 기본적으로 확보하고 심층 분석해야 할 주요 로그 유형 예시는 다음과 같다.

No	구분	보존 대상
1	개인정보처리시스템	접속기록(계정, 접속일시, 접속지 IP, 처리한 정보주체 정보, 수행업무), 권한 부여·변경·말소 기록 등
2	웹/애플리케이션	웹 서버 접속로그, 오류 로그, WAS 로그, API 로그 등
3	데이터베이스	DB 감사로그, 쿼리 로그, 접속 이력, 계정/권한 변경 이력 등
4	네트워크/보안장비	방화벽, IPS/IDS, WAF, VPN 접속 로그 등
5	서버/엔드포인트	운영체제 로그(윈도우 이벤트로그, 리눅스 시스템 로그), 백신 탐지 로그
6	인증 시스템	AD/LDAP 인증 로그, SSO 로그, 계정 잠금·비밀번호 변경 이력
7	클라우드	API 호출 로그(CloudTrail, Activity Log 등), 스토리지(S3) 액세스 로그, 네트워크 흐름 로그(VPC Flow Logs 등)
8	이메일·협업도구	메일 발송·수신 기록, 대용량 첨부 발송 이력, 웹메일·개인 클라우드 접속 기록

- 개인정보 유출등 신고 이후 개인정보보호위원회 등의 조사 과정에서 아래 자료의 제출이 요구될 수 있으므로, 유출등 대응 초기부터 체계적으로 정리·보존한다.
  - 유출등 개요 자료 : 유출등 인지 경위, 유출등 일시·기간, 유출등 항목·규모, 원인분석 결과, 시간대별 대응 조치 내역 등 타임라인
  - 증거 자료 : 보존 대상 로그, 디스크 이미지, 악성코드·웹쉘 등 공격 도구 사본, 보안 장비 로그, 자체 분석 보고서
  - 안전조치 이행 증적 : 내부관리계획, 접근권한 부여·변경·말소 내역, 접속기록 보관·점검 내역, 비인가 접근통제 현황 및 내역, 암호화 적용 현황, 취약점 점검·조치 결과 등 개인정보의 안전성 확보조치 기준 이행을 확인할 수 있는 자료

- 조치 결과 자료 : 정보주체 통지 내역(통지문, 발송 기록), 회수·삭제 조치 결과, 재발 방지 대책
- 위탁·클라우드 관련 자료 : 위·수탁 계약서, 수탁사 관리·감독 내역, CSP/MSP와의 책임분담 관련 자료

초동 분석 방법 및 사례

- 로그 분석은 유출등 경로·규모의 신속한 확정을 목표로, 유출등 지점에서 가까운 로그부터 우선 분석하고 주변 로그로 확장한다.
  - 유출등 지점 시스템의 로그 : 개인정보처리시스템 접속기록, 웹서버·DB 로그 등 유출등 정보를 직접 보유·처리한 시스템의 기록
  - 인증·계정 로그 : 비정상 로그인, 권한 상승, 계정 생성·변경 이력 → 공격자(또는 내부자)의 계정 사용 범위 확정
  - 네트워크 경계 로그 : 방화벽, WAF, VPN, 프록시 → 침입 경로와 데이터 반출(외부 전송량) 확인
- 해킹에 의한 유출등 지점 분석 사례

  유출등 의심 기간의 요청을 대상으로 공격 구문이 포함된 비정상 파라미터, 응답 크기가 비정상적으로 큰 요청을 우선 식별한다. 특히, 정상 사용자라면 거치는 화면·API 호출 순서(로그인 → 조회 등)를 건너뛴 요청이 있는지 확인한다.

  또한, 자동화 및 대량 수집 징후 파악을 위해 동일 IP·세션·계정에서 단시간 내 대량 요청 발생 여부, 파라미터 값(회원번호, 게시글 번호 등)을 기계적으로 순차 증가시키며 반복 호출하는 크롤러·매크로 징후를 분석한다. 최근에는 공격자가 IP를 다수로 분산시켜 IP 기준 임계치 탐지를 우회하는 사례가 나타나고 있다. 이 경우 세션 ID, 계정, User-Agent, 요청 패턴(정상 사용자와 비교 등) 기준으로 재집계하여 평시 대비 요청량을 비교한다.

  로그 유형별 유출등 지점 분석 예시는 다음과 같다.

구분	확인 사항 예시
웹/애플리케이션	- DB 오류 메시지를 통해 공격 구문 및 타겟 테이블·컬럼 파악 - 대용량 다운로드 타임아웃, 권한 접근 실패 이력으로 역추적 - 접근 로그에 남지 않는 요청 본문(POST body) 확인
데이터베이스	- 대량 조회 쿼리 여부, 특히 조건 없는 전체 조회나 개인정보 컬럼 일괄 조회 - 업무시간 외·비정상 시간대의 접속과 쿼리 - 평소 사용하지 않는 계정·출발지 IP에서의 접속 - 시스템 테이블·스키마 정보 조회 - 데이터 반출 기능(파일 내보내기, DB Link 등) 사용 이력을 분석 - 감사 로그가 없는 경우 WAS의 쿼리 로그, DB 접근제어 솔루션 로그 분석
네트워크·보안장비	- 방화벽 로그에서 내부 → 외부 대량 전송 확인 - 다수의 해외 IP 대역과의 통신, 아웃바운드 연결 포트 사용 확인 - WAF·IPS 탐지 이력은 공격 시도 시점과 차단·통과 여부를 대조하여 실제 침투 성공 시점을 특정하는 데 활용
서버·엔드포인트	- 로그온 이벤트(성공, 실패, 특히 원격 로그온 유형 확인) - 계정 생성/권한 변경 로그 확인 - 프로세스 생성 기록 확인 - 명령어(파워셸, 리눅스 쉘 실행) 로그 확인
클라우드	- 비정상 출발지(미사용 국가·익명화 IP)에서의 API 호출 - 계정정보 조회, 자원 목록 조회 등에 이은 데이터 접근 호출 - 액세스 키 생성·권한 변경 등 지속성 확보 행위 - 클라우드 데이터 저장소 및 스토리지 객체 대량 조회·다운로드

- 로그 간 시각 동기화(타임존, NTP 오차)를 확인하여 통합 타임라인을 작성하고, 침입 → 정찰 → 권한 획득 → 유출등 → 흔적 삭제의 단계별로 사건을 재구성한다. 분석 결과 확인된 유출등 규모·항목은 유출등 통지·신고 내용에 즉시 반영한다.
- 유출된 데이터가 다크웹 등 외부 게시된 장소에서 확인된 경우 샘플 데이터에 포함된 최신 레코드의 가입일·수정일이 유출등 시점의 하한이 될 수 있으며, 샘플 데이터를 자사 DB와 대조하여 유출등 테이블을 특정할 수 있다.

■ 유출등이 된 개인정보 회수·삭제

- 유출등이 된 개인정보가 외부에 유통되고 있는지 확인하고, 회수·삭제 등의 조치를 통해 추가 피해 가능성을 최소화한다.
  - 다크웹·해킹포럼·파일공유 사이트 등에 대한 유통 모니터링을 실시한다.
  - 유통이 확인된 경우 게시 데이터가 실제 자사에서 유출된 것인지 확인하고 해당 사이트 운영자에게 삭제를 요청한다. 필요시 수사기관과 협력한다.
  - 회수·삭제 결과는 기록하여 보관한다.

개인정보 유출등 유형별 대응 예시

1. 내부자가 유출등을 한 경우

개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역 확인
개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등이 정상적인지 여부 등을 확인하고, 비정상적인 접속인 경우 우회 경로를 확인하여 접속 차단
개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출등 여부 확인
개인정보 유출등에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 필요시 수사기관 등과 협조하여 유출등이 된 개인정보를 회수하기 위한 방법 강구

2. 이메일 오발송에 의한 경우

이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일 삭제 요청
메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일서버 운영자에게 관련 파일 삭제 요청

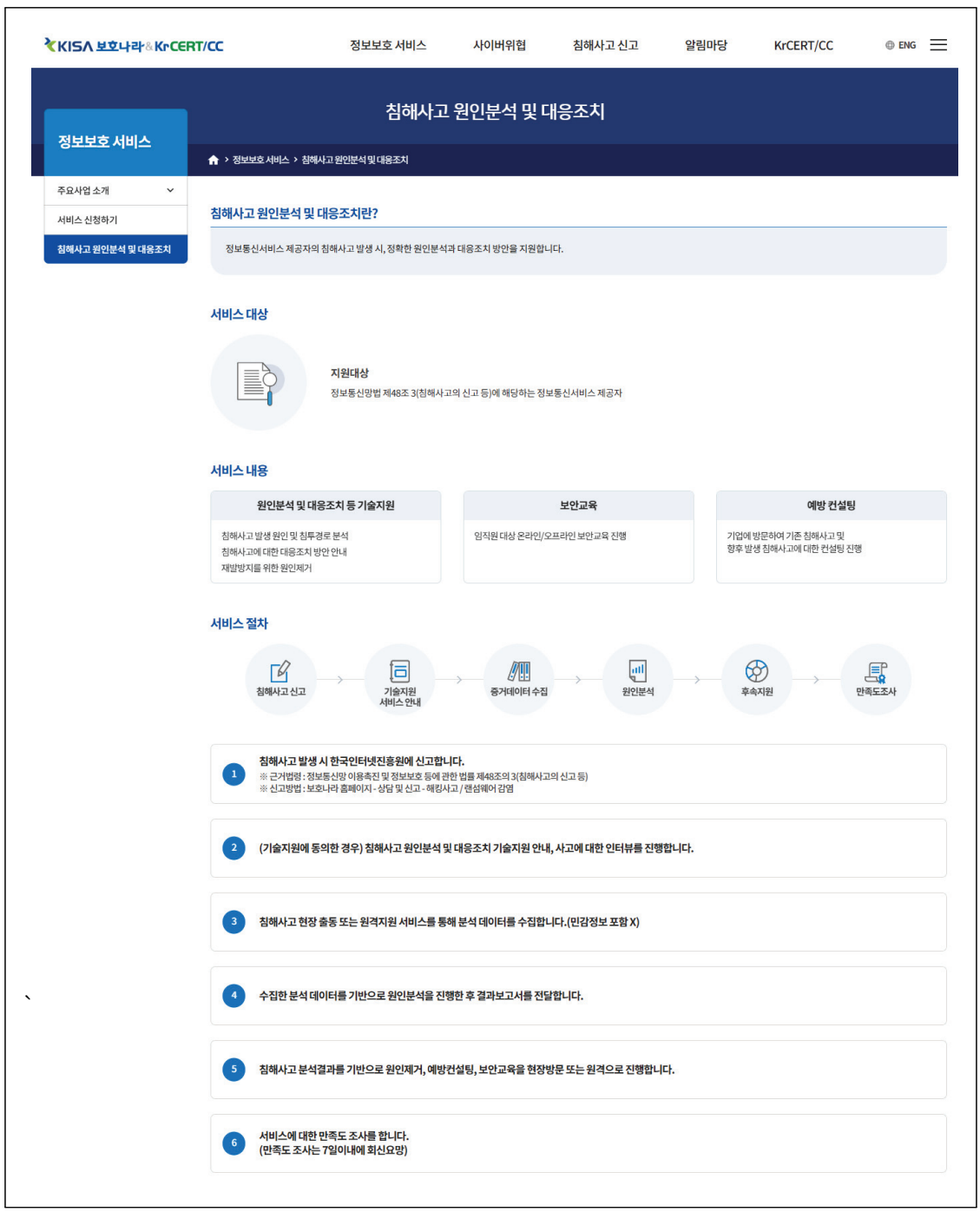
3. 개인정보 노출에 의한 경우

(검색엔진을 통한 노출의 경우) 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 인증 절차 추가 및 로봇배제 규칙 적용 등 외부 접근 차단
(시스템 오류로 인한 노출의 경우) 소스코드 오류, 서버 설정 오류 등 개인정보가 노출된 원인이 된 시스템 오류를 파악하여 수정
(개인정보취급자 부주의로 인한 노출의 경우) 게시글 및 첨부파일 내 개인정보 노출 부분을 마스킹 처리하여 게시

외부 전문기관 지원

- 자체 대응이 곤란하거나 침해사고가 중대한 경우 외부 전문기관의 기술지원을 요청한다.
  - 중소기업의 경우 한국인터넷진흥원(KISA)에서 제공하는 침해사고 원인분석 및 대응조치(boho.or.kr)를 이용할 수 있다.
  - 디지털포렌식 분석, 법률 자문 등이 필요한 경우 전문업체와 협력한다.

※ 기타 개인정보 유출등 예방은 개인정보의 안전성 확보조치 기준 안내서 등을 참고한다



침해사고 원인분석 및 대응조치(boho.or.kr)

Ⅲ

개인정보 유출등·유출등의 가능성 통지

Ⅲ 개인정보 유출등·유출등의 가능성 통지

1 개인정보 유출등의 통지

■ 통지 요건

- 통지 의무
  - 개인정보처리자는 개인정보가 유출등이 된 사실을 알게 된 경우 정보주체에게 통지하여야 한다.
  - 유출등이 된 정보주체가 단 1명인 경우에도 통지하여야 하며, 유출등 규모가 작다는 이유로 통지를 생략할 수 없다.
- 적용 제외
  - 가명정보가 유출등이 된 경우에는 적용되지 않는다(개인정보 보호법 제28조의7).

※ 가명정보는 그 자체로 정보주체를 식별할 수 없으므로, 통지를 이행하기 위해서는 추가정보와의 결합을 통한 재식별 과정이 불가피하며, 이는 가명처리 제도의 목적에 반하는 결과를 초래하므로 적용 대상에서 제외된다.

통지 의무를 이행하지 않은 사례

- ○○정보통신사가 개인정보취급자의 실수로 정보주체 10여 명의 인적사항이 담긴 개인정보파일을 이메일에 첨부하여 다른 사람에게 오발송하였으나, 해당 파일에 포함된 정보주체에게 유출등 통지를 하지 않은 경우
  ⇒ 단 1명의 개인정보가 유출등이 된 경우에도 해당 정보주체에게 유출등 통지하여야 한다.

통지 기한

- 개인정보처리자는 유출등의 사실을 알게 된 때부터 72시간 내에 정보주체에게 통지하여야 한다.

  ※ 개인정보처리자는 유출등을 인지한 시점을 객관적 자료(민원 접수 일시, 유출등 제보·확인 일시, 침해행위자의 협박 메일 수신·확인 일시 등)로 입증할 수 있어야 한다.

  ※ 유출등을 알게 된 때로부터 72시간을 초과하여 통지하는 경우, 개인정보처리자는 지연 사유 및 정당성을 객관적인 자료로 소명할 수 있어야 한다.

- 다음의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 즉시(적어도 72시간 이내) 정보주체에게 알릴 수 있다.

  - 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
  - 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

통지 지연 사례

사례 1

- 크리덴셜 스터핑 공격으로 회원정보가 유출된 사실을 인지하였고, 이후 분석을 통해 직원정보도 유출된 사실을 충분히 알 수 있었음에도 정당한 사유 없이 직원을 대상으로 2개월을 경과하여 유출등 통지한 경우

사례 2

- ○○기관으로부터 개인정보처리자의 개인정보가 저장된 DB 테이블이 다크웹, 해커의 서버에서 발견되었고 개인정보 유출등 신고 및 통지할 것을 안내하는 내용의 메일을 수신함. 해당 메일을 통해 다크웹, 해커의 서버에서 발견된 정보가 회원정보임을 확인하는 등 유출을 인지하였음에도, 72시간을 경과하여 유출등 통지한 경우

사례 3

- 해커의 공격으로 20여 건의 결제정보가 유출된 사실을 이미 파악하고 있었고, ○○기관으로부터 수신한 안내 메일에도 유출된 정보가 데이터베이스 내 ○○테이블로 확인된다는 내용이 기재되어 있었으며 해당 ○○테이블에 회원의 이름·주소·생년월일·휴대전화번호 등이 보관되고 있었음에도, 해당 메일에 첨부된 근거자료가 웹 서버 접속 로그 2줄에 불과하여 유출 항목과 대상자 파악이 곤란하였다는 이유로 4일을 경과하여 유출등 통지한 경우

사례 4

- 해커에 의해 개인정보가 유출된 사실을 확인한 후 경찰청에 신고하였으나, 수사관으로부터 해커가 검거될 때까지는 유출등 통지를 유보해 달라는 구두 요청을 받고 30일 이상 통지를 지연한 경우

  ⇒ 해커 검거를 통해 유출된 개인정보를 회수하기 위해 경찰청으로부터 필요한 최소한의 기간 동안 유출등 통지 보류를 요청받은 경우에는 개인정보보호위원회에 유출등 신고 후 협의하여야 하며, 그 사유를 소명하여야 한다.

통지 항목

- 유출등 통지에는 다음 각 호의 항목이 모두 포함되어야 한다.

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
6. 손해배상과 법정손해배상의 청구 및 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보

통지 항목 누락 사례

사례 1

– 정보주체에게 유출등 통지를 하면서 제목을 '개인정보 유출 사고에 대한 사과 말씀'으로만 표기하고 유출등 대상자를 '12만여 명'으로 기재하는 데 그쳐, 통지를 받은 정보주체가 자신의 개인정보가 유출등 된 것인지 판단할 수 없도록 통지한 경우

사례 2

– 유출등이 된 개인정보 항목 중 성명·생년월일·연락처·이메일 주소·ID·주민등록번호만 기재하고, 휴대전화번호·계좌번호·○○번호 등 개인 식별성이 높은 나머지 항목을 '등'으로 생략하여 통지한 경우

유출등 통지문 예시

개인정보 유출등 사실을 통지해 드리며, 깊이 사과드립니다.

① **고객님의 개인정보는 ○○○년 ○○월 ○○일 해킹에 의해 홈페이지 내 악성코드가 삽입**되어 ○○건이 유출된 것으로 확인되었습니다. 유출된 정확한 일시는 ○○에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.

② **유출된 개인정보의 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목**입니다.

③ 유출 사실을 인지한 후 **해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당 IP와 우회 접속한 IP를 차단**하고, 추가적인 **홈페이지 취약점 점검 및 보완 조치**를 하였습니다. 더불어 **침입방지시스템을 추가 도입하여 24시간 모니터링**을 수행하고 있습니다.

이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 파밍 등 **2차 피해의 우려가 있으므로** 혹시 모를 피해를 막기 위하여 아래와 같이 ④ **피해 최소화 조치를 취할 수 있음을 안내 드립니다.**

④ ▶ **피해 최소화 조치**

- **스미싱·피싱 문자 및 메일 주의 :** 출처가 불분명한 링크 클릭이나 개인정보·금융정보 입력 요구에 응하지 않도록 주의하여 주시기 바랍니다.
- **명의도용 확인 :** 명의도용 방지 서비스(예 : 명의도용확인 서비스, 계정 신규 개설 알림 등)를 이용하여 본인 명의의 부정 이용 여부를 주기적으로 확인하여 주시기 바랍니다.
- **비밀번호 변경 :** 현재 사용 중인 비밀번호를 즉시 변경하시기 바라며, 특히 다른 웹사이트에서 동일한 비밀번호를 사용하고 계신 경우 해당 사이트의 비밀번호도 함께 변경하여 주시기 바랍니다.

[비밀번호 변경하기(링크)]
※ 메뉴 : 마이페이지 〉 회원정보 수정 〉 비밀번호 변경

⑤ **개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해 주시기 바랍니다.**

▶ **피해 등 접수 담당부서 : ○○○팀(Tel : 000-2345-0000)**
▶ **피해 등 접수 e-mail : ○○○○@oooo.co.kr**

⑥ 이번 개인정보 유출로 인하여 손해를 입으신 경우, 고객님께서는 다음과 같은 방법으로 권리를 구제받으실 수 있습니다.

▶ **손해배상 청구 : 개인정보처리자의 법 위반으로 인하여 손해를 입으신 경우 고의 또는 과실을 입증하지 않고도 손해액을 산정하여 회사를 상대로 민사소송(손해배상청구소송)을 제기하실 수 있습니다.**

▶ **법정손해배상 청구 : 개인정보처리자의 고의 또는 과실로 인한 개인정보 유출등이 인정되는 경우, 고의 또는 과실 및 실제 손해액을 입증하지 않고도 민사소송 절차를 통해 손해배상을 청구하실 수 있습니다.**

▶ **분쟁조정 신청 : 개인정보 침해로 인한 분쟁에 대하여 개인정보 분쟁조정위원회에 조정을 신청하실 수 있습니다. kopico.go.kr(1833-6972)**

(주) ○○○ 대표이사 ○○○

⑦ 개인정보 유출 여부 조회하기

■ 개인정보 유출등 통지문 작성 준수사항

① 개인정보 유출등이 발생한 사항과 확인된 유출등 건수를 누구나 이해할 수 있게 상세하게 설명
※ 잘못된 사례 : '일부 고객, 회원정보 일부' 등

② 유출등이 된 개인정보 항목은 누락 없이 모두 나열
※ 잘못된 사례 : '등'으로 생략하거나, 회사전화번호, 집전화번호를 '전화번호'로 통칭

③ 개인정보처리자의 대응 조치 내용
접속경로 차단 등 해킹 방면 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명

④ 정보주체가 취할 수 있는 피해 최소화 방법
유출등이 된 개인정보의 항목, 유출등 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내한다.(예 : 보이스피싱, 피싱메일, 불법 TM, 스팸문자 주의 등)
피해 최소화 조치의 하나로, 비밀번호 변경 방법 등 정보주체가 할 수 있는 계정 보호조치를 함께 안내할 수 있음
(예 : 2단계 인증(추가 인증) 설정, 해외 IP 로그인 제한 등)

⑤ 정보주체가 상담 등을 접수할 수 있는 부서 및 연락처
전담처리부서 안내를 원칙으로 하되, 대량 유출등으로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

⑥ 손해배상과 법정손해배상의 청구 및 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보를 안내

⑦ 정보주체가 자신의 개인정보 유출등 여부를 조회할 수 있도록 절차를 마련할 수 있음

● 유출등 통지하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 통지하고, 추가로 확인되는 내용은 확인되는 즉시 통지한다.

※ 구체적 사실관계 파악을 이유로 정보주체에게 유출등 사실 통지를 지연하는 경우 개인정보 보호법 제34조 제1항 위반에 해당할 소지가 있다.

통지 방법

● 개인정보처리자는 정보주체에게 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 개별 통지하여야 한다.

※ 통지 시 정보주체가 실제 확인할 수 있도록 이용 빈도가 높은 방법을 우선 활용하는 것이 바람직하다. 휴대전화번호를 보유하고 있는 경우에는 전화통화 및 문자 등을 활용하고, 해당 방법으로 통지하기 곤란한 경우에는 전자우편, 팩스, 우편 등의 방법을 활용한다.

● 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 인터넷 홈페이지에 30일 이상 게시하는 것으로 개별 통지를 갈음할 수 있다.

- 인터넷 홈페이지를 운영하지 않는 경우에는 사업장 등 보기 쉬운 장소에 30일 이상 게시하는 방법으로 통지할 수 있다.

※ 홈페이지에 게시할 때에는 '개인정보 유출등 안내' 등 정보주체가 내용을 쉽게 인식할 수 있는 제목을 사용하고, 법에서 정한 통지 내용이 모두 포함되어야 한다.

통지 방법이 잘못된 사례

사례 1

- 유출등 인지 당시에는 유출등이 된 이용자가 특정되지 않아 홈페이지 공지사항을 통해 유출등 통지를 하였으나, 이후 조사 과정에서 유출등이 확인된 이용자 ○명에 대하여 개별적으로 유출등 통지를 하지 않은 경우

⇒ 정보주체가 특정되지 않아 부득이하게 공지로 갈음하였더라도, 이후 대상자가 확인되었다면 그 시점에 확인된 정보주체에게 개별 통지를 하여야 한다.

사례 2

- 다크웹에 공개된 파일명 및 데이터 구조가 인수 전 사용하던 舊시스템의 정보와 일치하는 것으로 확인되었고, 공개된 성명·생년월일·주소 등 개인정보 중 現시스템의 개인정보와 일치하는 정보주체 ○명이 특정되었음에도, 홈페이지 공지만 실시하고 해당 정보주체에게 70여 일이 지나서야 유출등 통지를 한 경우

⇒ 리브랜딩·시스템 전환 이전에 수집된 개인정보라도 개인정보처리자의 지위에서 처리하는 개인정보라면 통지 의무의 대상이며, 현재 보유 중인 정보와 대조하여 개별 통지를 하여야 한다.

FAQ 질의 응답

Q1 **정보주체의 연락처(휴대전화번호, 유선번호 등), 주소, 이메일주소를 알고 있으나, 해당 연락 수단으로 개별 통지 진행하지 않고 홈페이지에 30일 이상 게시하는 것으로 갈음할 수 있나요?**

답변 홈페이지 게시로 갈음할 수 없습니다.

연락처를 알 수 없는 등 정당한 사유가 있는 경우에 한해 개별 통지를 홈페이지 게시로 갈음하는 것이 허용됩니다.

유출등 통지 제도는 정보주체가 유출등 사실을 신속히 인지하고 2차 피해를 스스로 방지할 수 있도록 하는 데 목적이 있습니다. 홈페이지 게시는 정보주체가 직접 접속해야만 확인할 수 있어 이 목적을 충분히 달성하기 어려우므로, 법령은 이를 개별 통지가 불가능한 경우의 보충적 수단으로만 인정하고 있습니다.

따라서 휴대전화번호·유선번호·주소·이메일주소 등 정보주체의 연락 수단을 보유하고 있는 경우에는 이를 활용하여 개별 통지를 실시하여야 합니다.

Q2 **개인정보가 랜섬웨어에 감염되었거나 해커가 DB에 접근하여 개인정보를 삭제하는 등 개인정보가 영구적으로 삭제된 훼손 상태입니다. 따라서 정보주체의 연락처를 알 수 없습니다. 어떻게 유출등 통지를 해야 하나요?**

답변 랜섬웨어 감염이나 해커의 삭제 행위로 개인정보(성명, 연락처 등)가 훼손되어 개인정보처리자가 더 이상 이를 보유하고 있지 않은 경우에는, 정보주체 개개인의 연락처 자체를 확인할 방법이 없으므로 정보주체의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에 해당합니다. 이 경우 개인정보처리자는 자신의 인터넷 홈페이지에 30일 이상 게시하는 방법으로 개별 통지를 갈음할 수 있으며, 인터넷 홈페이지를 운영하지 않는 경우에는 사업장 등 보기 쉬운 장소에 30일 이상 게시하는 방법으로 통지할 수 있습니다.

Q3 **아이디, 비밀번호 등만 유출등이 되고 이메일주소 등 연락처는 유출등이 되지 않은 이용자에 대해서는 개별 통지를 생략해도 되나요?**

답변 아이디, 아이디+일방향 암호화된 비밀번호 등만 유출등이 된 경우라도 별도 보관 중인 연락처 정보 등을 활용하여 개별 통지를 실시하여야 합니다.

2 개인정보 유출등의 가능성 통지

통지 요건

- 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우 정보주체에게 개인정보 유출등의 가능성을 통지하여야 한다.
- (요건 ①) 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 불법적인 접근이 발생하여 개인정보 유출등이 의심되는 정황이 있으나 그 개인정보의 정보주체를 특정하기 곤란한 경우

※ 의심되는 정황이란 단순한, 취약점의 존재나 공격 시도를 의미하는 것이 아니라 불법적인 접근의 성공, 개인정보 테이블에 대한 비정상 질의, 비인가 대량 조회·다운로드 또는 외부 전송 흔적 등 객관적인 자료에 비추어 개인정보가 유출등이 되었을 개연성은 인정되지만, 실제 유출등 여부·범위 또는 대상 정보주체를 확정하기 곤란한 상황을 말한다.

요건 ① 유출등 가능성 통지 예시

예시 1 SQL Injection 공격으로 개인정보 테이블을 대상으로 한 비정상 질의(query)가 실행되고 해당 질의가 성공적으로 처리되는 등 개인정보 유출등이 의심되는 정황이 있으나, 실제 조회 결과 반환 값에 따라 유출등이 된 구체적인 정보주체를 특정하기 곤란한 경우

예시 2 해커가 회원 조회 페이지의 요청 파라미터를 변조하여 타인의 개인정보 조회를 시도하고 해당 요청이 정상 처리된 것으로 보이는 등 개인정보 유출등이 의심되는 정황이 있으나, 회원번호 등 조회 대상 식별 값이 POST 방식 등으로 로그에 저장되지 않도록 설정되어 조회된 정보주체를 특정하기 어려운 경우

예시 3 해커가 개인정보를 처리하는 관리자 페이지 등에 권한 없이 로그인하여 개인정보 조회 페이지, 개인정보 조회 기능 등에 접근하는 등 개인정보 유출등이 의심되는 정황이 있으나, 조회된 정보주체를 특정하기 곤란한 경우

예시 4 퇴직자가 퇴직 직전에 회사 외부에서 개인 컴퓨터로 원격 접속하여 업무 목적과 무관하게 단시간 내 수만 건의 고객정보를 조회 및 다운로드한 사실에 대한 정황은 확인되었으나, 화면 단위 조회기록과 다운로드 기록만 남아 있어 실제 조회·다운로드된 정보주체를 특정할 수 없는 경우

예시 5 네트워크 트래픽 분석 결과 개인정보 파일이 외부 서버로 전송된 사실은 확인되었으나, 해당 파일이 해커가 비밀번호를 설정한 압축파일 형태여서 원본 데이터를 복원·확인하여 정보주체를 특정할 수 없는 경우

위 예시와 같이 유출등이 된 정보주체를 특정할 수 없는 경우에는 해당 침해행위가 미칠 수 있었던 정보주체 전체를 대상으로 유출등의 가능성을 통지한다. 다만, 기술적·객관적 분석을 통해 제3자가 접근 및 유출등이 가능한 정보주체의 범위가 한정됨을 입증할 수 있는 경우에는 해당 범위 내의 정보주체를 대상으로 개인정보 유출등에 대한 가능성 통지를 할 수 있다.

● (요건 ②) 개인정보가 개인정보 보호 법령을 위반하여 제3자에 의해 거래되는 등 일부 개인정보가 유출등이 된 사실이 확인된 경우로서 다른 정보주체에 관한 개인정보도 유출등이 되었을 수 있다고 인정되는 경우

요건 ② 유출등 가능성 통지 예시

예시 1 해커가 다크웹에서 전체 회원정보 판매글을 올리면서 일부 샘플 회원정보 1만 건을 공개하였고, 컬럼 구성·식별값 부여 형식 및 표본 대조 결과가 개인정보처리자의 데이터베이스와 일치하여 해당 테이블로부터 유출된 사실이 확인되었으나, 공개된 1만 건 외에 추가로 유출등이 된 범위는 확인할 수 없는 경우

- 공개가 확인된 정보주체에 대하여는 유출등 통지를, 동일 테이블 등 해커가 접근할 수 있었던 그 밖의 정보주체에 대하여는 유출등 가능성 통지를 할 수 있다.

● 유출등의 가능성이 있는 경우로 보지 않는 경우

- 객관적으로 개인정보 유출등의 가능성이 없는 경우에는 정보주체에게 알리지 않을 수 있다.

유출등의 가능성이 있는 경우로 보지 않는 예시

예시 1 SQL Injection 공격으로 개인정보 테이블을 대상으로 한 비정상 질의(query) 시도가 있었으나, 공격 재현 검증 및 로그 분석 결과 공격에 사용된 계정이 개인정보 테이블에 대한 권한을 보유하지 않아 개인정보의 조회·변경·삭제 등이 이루어지지 않았음이 확인되는 등 유출등이 의심되는 정황이 없는 경우

예시 2 해커가 개인정보를 처리하는 관리자 페이지 등에 로그인하였으나, 해커의 접속기록을 분석한 결과 개인정보 조회 페이지, 개인정보 조회 기능 등에 접근하지 않아 개인정보 유출등이 의심되는 정황이 없는 경우

예시 3 다크웹에 개인정보처리자의 회원정보라는 샘플 1만 건이 공개되었으나, 샘플에 개인정보처리자가 수집하지 않는 항목이 포함되어 있고, 컬럼명과 정보주체 식별값의 부여 형식이 상이하며, 샘플의 데이터를 개인정보처리자의 회원정보와 비교한 결과 일치하지 않는 등 해당 개인정보처리자로부터 유출등이 되었다는 정황이 없는 경우

예시 4 해커가 개인정보처리자의 개인정보를 확보하였다고 주장하며 금전을 요구하였으나, 샘플 데이터의 제시 요구에 응하지 않았고 주장한 규모가 실제 보유 회원 수와 현저히 상이하며, 개인정보처리자가 접속기록·방화벽 등의 기록을 분석한 결과 개인정보 유출등이 없는 것으로 확인된 경우

예시 5 개인정보취급자 1인의 계정이 탈취되어 해당 계정으로 조회한 정보주체 100명의 개인정보가 거래되고 있는 사실이 확인되었으나, 해당 계정에 부여된 권한이 담당 업무 범위로 한정되어 있고 접속기록 상 그 밖의 정보주체에 대한 조회 이력이 없는 경우
(※ 확인된 정보주체 100명에 대하여는 유출등의 통지를 하여야 함)

● 적용 제외

- 유출등 통지와 동일하게 가명정보가 유출등이 된 경우에는 적용되지 않는다(개인정보 보호법 제28조의7).

■ 통지 기한

- 개인정보처리자는 유출등의 가능성을 알게 된 때부터 72시간 내에 정보주체에게 통지하여야 한다.
  - 요건 ①의 경우 해당 불법적인 접근을 알게 된 때를 말하며, 요건 ②의 경우 해당 사실을 알게 된 때를 말한다.

    ※ 개인정보처리자는 유출등의 가능성을 인지한 시점을 객관적 자료(민원 접수 일시, 유출 제보·확인 일시, 침해행위자의 협박 메일 수신·확인 일시 등)로 입증할 수 있어야 한다.

    ※ 유출등의 가능성을 알게 된 때로부터 72시간을 초과하여 통지하는 경우, 개인정보처리자는 지연 사유 및 정당성을 객관적인 자료로 소명할 수 있어야 한다.

- 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우에는 해당 사유가 해소된 후 즉시(적어도 72시간 이내) 정보주체에게 통지해야 한다.

  ※ 유출등의 가능성 통지는 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 긴급한 조치가 필요하다는 사유로는 지연할 수 없다. 이 점에서 유출등의 통지와 차이가 있다.

- 유출등 가능성의 통지 기한 내에 개인정보가 실제로 유출등이 된 사실을 확인한 경우에는 유출등의 통지를 하는 것으로 유출등 가능성의 통지를 갈음할 수 있다.

■ 통지 항목

- 유출등 가능성 통지에는 다음 각 호의 항목이 포함되어야 한다.

  1. 유출등의 가능성이 있는 개인정보의 항목
  2. 유출등이 있었을 것으로 의심되는 시점과 그 경위
  3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적 정보
  4. 개인정보처리자의 대응조치 및 피해 구제절차
  5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
  6. 유출등의 여부가 확정될 경우 추가 통지를 하겠다는 사실

  ※ 유출등의 가능성 통지는 유출등 사실 확정 전 단계의 통지인 만큼, 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보(제34조제1항제6호에 따른 유출등의 통지 사항)는 포함하지 않고, 향후 유출등 여부가 확정될 경우 추가 통지가 이루어진다는 사실을 포함하여야 한다.

- 유출등의 가능성 통지를 하는 경우 정보주체에게 불필요한 혼란이나 과도한 불안을 초래하지 아니하도록 통지 취지와 한계를 명확히 밝혀야 한다.

유출등의 가능성 통지문 예시

개인정보 유출등 가능성을 안내드립니다.

① **당사 개인정보처리시스템에서 ○○○년 ○○월 ○○일경 해킹에 의해 홈페이지 내 악성코드가 삽입되어 해커가 개인정보를 조회·추출하는 등의 유출등 정황이 확인되었습니다.** 다만, 현재까지 조사 결과 유출등이 된 정보주체를 특정하기 곤란 상황으로, 귀하를 포함하여 해당 시스템을 이용하신 고객님들께 개인정보 유출등 가능성을 통지 드립니다.

② **유출등이 되었을 가능성이 있는 개인정보의 항목은 귀하께서 당사에 등록·보유하고 계신 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호**이며, 실제 유출등 여부 및 항목은 조사 결과에 따라 달라질 수 있습니다.

③ 당사는 이상행위를 인지한 후 즉시 해당 **계정·접근경로에 대한 접속을 차단**하고, 관련 로그를 보전하는 한편, 홈페이지 **취약점 점검 및 보완 조치를 실시하였습니다. 더불어 침입탐지·방지시스템을 통한 24시간 모니터링을 강화하여 추가 피해 발생 여부를 확인**하고 있습니다.

④ 이번 **이상행위로 인해 개인정보가 유출등이 되었을 경우 웹사이트 명의도용, 보이스피싱, 파밍 등 2차 피해가 발생할 우려가 있으므로**, 혹시 모를 **피해를 예방하기 위하여, 출처가 불분명한 전화·문자·이메일에는 응답하거나 링크를 클릭하지 않으시기 바랍니다.**

⑤ 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 **아래 피해 등 접수 담당부서로 연락해 주시기 바랍니다.**

▶ 피해 등 접수 담당부서 : ○○○팀(Tel : 000-2345-0000)
▶ 피해 등 접수 e-mail : ○○○○@oooo.co.kr

⑥ 향후 수사 및 조사를 통해 **유출등이 된 정보주체 및 항목이 특정되는 경우, 이를 즉시 개별 통지하여 드리겠습니다.**

(주) ○○○ 대표이사 ○○○

① 유출등이 있었을 것으로 의심 또는 인정되는 시점과 그 경위 설명

② 유출등의 가능성이 있는 개인정보의 항목 나열
개인정보의 항목은 누락없이 모두 나열하여야 함
※ 잘못된 사례 : '등'으로 생략하거나, 회사전화번호, 집전화번호를 '전화번호'로 통칭

③ 개인정보처리자의 대응조치 내용
접속경로 차단 등 해킹 방면 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명

④ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적 정보
유출등이 된 개인정보로, 해당 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예 : 보이스피싱, 피싱메일, 불법 TM, 스팸문자 주의 등)

⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
전담처리부서 안내를 원칙으로 하되, 대량 유출등으로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

⑥ 유출등의 여부가 확정될 경우의 추가 통지를 하겠다는 사실 설명

통지 방법

- 통지 방법은 개인정보 유출등의 통지와 동일하므로 개인정보 유출등의 통지 방법을 참고한다.

추가 통지

- 유출등 가능성을 통지한 후 해당 정보주체에 대한 유출등의 여부가 확정된 경우에는 그 결과를 다음과 같이 추가로 통지하여야 한다.
  - 해당 정보주체에 대하여 유출등이 된 사실을 알게 된 경우 : 72시간 이내에 유출등 통지를 해야 한다.
    ※ 유출등의 통지에 관하여는 유출등의 통지 부분을 참고한다.
  - 개인정보가 실제로 유출등이 되지 않은 사실을 확인한 경우 : 즉시(적어도 72시간 이내) 해당 정보주체에게 유출등이 되지 않았다는 사실을 통지하여야 한다.
    ※ 개인정보가 실제로 유출등이 되지 않은 사실을 확인한 경우의 통지 방법도 동일하므로, 유출등의 통지 방법을 참고한다.

Ⅳ

개인정보 유출등의 신고

Ⅳ 개인정보 유출등의 신고

■ 신고 요건

● 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우 개인정보 유출등의 신고를 하여야 한다.

- 1천 명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
- 민감정보 또는 고유식별정보가 유출등이 된 경우
- 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

참고 | 고유식별정보·민감정보의 정의

• 고유식별정보의 정의 (법 제24조제1항, 시행령 제19조)
- 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 다음 각 호의 어느 하나에 해당하는 정보를 말한다.
  1. 「주민등록법」 제7조의2제1항에 따른 주민등록번호
  2. 「여권법」 제7조제1항제1호에 따른 여권번호
  3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
  4. 「출입국관리법」 제31조제5항에 따른 외국인등록번호
  ※ 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 처리하는 경우는 제외

• 민감정보의 정의(법 제23조제1항, 시행령 제18조)
- 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 각 호의 어느 하나에 해당하는 정보
  1. 유전자검사 등의 결과로 얻어진 유전정보
  2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
  3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보,
  4. 인종이나 민족에 관한 정보
  ※ 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 처리하는 경우는 제외

FAQ 질의 응답

Q1 시스템 오류 또는 담당자 실수로 1천명 미만의 개인정보가 유출되었습니다. (민감정보·고유식별정보 미포함) 유출등 신고해야 하나요?

답변 유출등 신고 요건에 해당하지 않습니다.

개인정보 유출등 신고 요건은 ① 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우, ② 민감정보 또는 고유식별정보가 유출등이 된 경우, ③ 해킹 등 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우 중 어느 하나에 해당할 때 발생합니다.

권한 없는 제3자가 파라미터 변조 등 개인정보처리시스템의 취약점을 이용하여 정상적이지 않은 방법으로 개인정보에 접근한 경우, 또는 개발자 도구에만 노출되는 응답값(response)의 개인정보를 크롤링하여 다량의 개인정보를 탈취한 경우에는 외부로부터의 불법적인 접근으로 볼 수 있습니다. 다만, 정보주체가 검색엔진 등을 통해 정상적으로 서비스를 이용하는 과정에서 개인정보처리시스템의 오류로 인해 의도치 않게 타인의 개인정보를 조회한 경우는 시스템 오류로 볼 수 있습니다.

시스템 오류 또는 담당자 실수로 인한 유출등이면서 1천명 미만이고 민감정보·고유식별정보에도 해당하지 않는 경우에는 위 3가지 요건 중 어느 것에도 해당하지 않으므로 신고 요건에 해당하지 않습니다.

Q2 개인정보의 처리를 위탁받아 위탁사들의 개인정보처리시스템을 운영 중인 대형 수탁사입니다. 운영 중인 개인정보처리시스템의 취약점으로 인해 동일 경위로 다수의 위탁사 개인정보가 유출되었습니다. 위탁사가 모두 개별적으로 유출등 신고해야 하나요?

답변 원칙적으로 위탁자인 개인정보처리자는 유출등 신고 의무가 있습니다. 다만, 수탁사가 해당 위탁사들을 명시하여 기재한 후 일괄 신고하는 것으로 개별 유출등 신고를 갈음하는 것으로 볼 수 있습니다.

이러한 일괄 신고는 수탁사가 운영하는 개인정보처리시스템의 취약점으로 인해 다수의 위탁사에서 동일한 경위로 수탁받은 개인정보가 유출된 경우에 적용됩니다. 다만 위탁사별로 유출의 원인이나 경위가 상이하거나, 수탁사가 수탁받은 업무 범위를 벗어난 사유로 유출이 발생한 경우 등에는 다르게 판단될 수 있습니다.

- 신고하지 않을 수 있는 경우
  - 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 아니할 수 있다.
    ※ 다만, 이 경우에도 정보주체에 대한 유출등 통지 의무는 있으므로 별도로 통지하여야 한다.

신고 기한

- 개인정보처리자는 유출등 사실을 알게 된 때부터 72시간 이내에 신고하여야 한다.
  ※ 유출등의 발생 시점과 인지 시점이 다른 경우, 인지 시점을 객관적 자료(민원 접수 일시, 유출 제보 일시, 해커의 협박 메일 발송·확인 일시 등)로 입증할 수 있어야 한다.
  ※ 유출등을 알게 된 때로부터 72시간을 초과하여 신고하는 경우, 개인정보처리자는 지연 사유 및 정당성을 객관적인 자료로 소명할 수 있어야 한다.
- 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 즉시(적어도 72시간 이내) 신고할 수 있다.

신고 사항

- 유출등 신고에는 다음 각 호의 사항이 포함되어야 한다.

  1. 유출등이 된 개인정보의 항목
  2. 유출등이 된 시점과 그 경위
  3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적 정보
  4. 개인정보처리자의 대응조치 및 피해 구제절차
  5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
  6. 손해배상과 법정손해배상의 청구 및 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보

- 유출등이 된 개인정보의 항목, 유출등이 된 시점과 그 경위에 관하여 구체적인 내용을 확인하지 못한 경우에는, 개인정보가 유출등이 된 사실과 그때까지 확인된 내용 및 그 외의 사항을 우선 신고하고, 추가로 확인되는 내용은 확인되는 즉시 신고하여야 한다.
  - 이때, 추가로 확인되는 내용을 신고할 경우에는 최초 신고에 대한 추가 신고임을 명시하여 신고한다.

입력 항목	작성 방법 및 예시
유출등이 된 개인정보의 항목 및 규모	• 유출등이 된 개인정보 항목을 모두 기재해야 하며, '등'과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 '전화번호'로 기재하여서는 안 됨 (예시) • 항목 : 아이디, 비밀번호, 이름, 휴대전화번호, 주소, 이메일주소, 계좌번호 • 유출등 규모도 현 시점에서 파악된 내용을 모두 작성 (예시) • 규모 : 총 1,004건 – ID, PW, 이름, 휴대전화번호, 주소 : 1,004건 – 이메일주소, 계좌번호 : 404건
유출등이 된 시점과 그 경위	• 유출등 시점, 인지 시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출등 경위와 인지 경위를 포함 (예시) • 유출 발생 시점 : 2026-08-01 14:30 • 유출 인지 시점 : 2026-08-03 10:00 • 유출 및 인지 경위 – [유출 경위] 홈페이지 콘텐츠관리시스템(CMS)의 외부 연동 API 서버에 대한 외부의 비인가 접속(웹쉘 공격 / SQL Injection)으로 인해 고객 데이터베이스 일부가 외부로 유출됨 – [인지 경위] 2026년 8월 3일 10:00경 서버 관리자 계정의 이상 접근 로그 및 정보 유출 정황을 인지하여 분석을 진행함
유출등 피해 최소화 대책, 조치 및 결과	• 개인정보 유출등 사실을 안 후 긴급히 조치한 내용과 향후 정보주체의 피해 구제를 위한 계획 및 절차를 기재 (예시) • 즉시 대응 조치 – [2026-08-03 10:30] 침입 경로로 확인된 외부 연동 API 서버 접속 차단 및 IP 접근 제한 조치 완료 – [2026-08-03 11:00] DB 관리자 비밀번호 변경 및 시스템 전반 취약점 점검 실시 • 피해 최소화 조치 – [2026-08-03 18:30] 2차 피해 안내 상담 창구(CS 센터) 설치 및 전담 인력 배치 운영 • 유출 통지 – [2026-08-03 18:30~19:30] 유출 대상 고객 전원에게 개인정보 유출 사실 개별 통지(SMS 및 이메일 발송) • 유출된 정보에 결제 비밀번호, 카드번호 등 금융 정보 및 주민등록번호는 포함되지 않음을 확인함

입력 항목	작성 방법 및 예시
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	• 개인정보 유출등으로 발생 가능한 스팸 문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해 정보주체가 할 수 있는 조치를 기재 (예시) • 정보주체(고객) 행동 요령 – 본인 확인을 요청하는 문자 메시지(SMS) 내 URL 링크 클릭 자제 – 당사 또는 택배사를 사칭한 스미싱·보이스피싱 전화 및 문자에 유의 – 회원 비밀번호 변경 권장(동일한 ID/PW를 사용하는 타 사이트 비밀번호 포함)
정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	• 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재 (예시) • 피해 발생 시 구제 절차 안내 – 당사 개인정보 유출 전담 대응 대표번호 : 02-XXXX-XXXX (평일 09:00~18:00) – 당사 전용 이메일 문의 : privacy@company.com

이해하기 어려운 신고내용 #1

유출된 개인정보의 항목 및 규모	파악 중
유출된 시점과 경위	2025.05.28 오전 모든 시스템 대상 해킹 사고 발생
유출피해 최소화 대책·조치 및 결과	피해 현황 및 사고 원인 조사 진행 중
정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차	파악 중

이해하기 어려운 신고내용 #2

유출된 개인정보의 항목 및 규모	ID, 이름, 이메일, 휴대폰 번호 등 5,293명
유출된 시점과 경위	몇 일 전 KISA에서 해킹 메일을 받아 알게 되었음
유출피해 최소화 대책·조치 및 결과	보안 전담 인력 또는 시스템 운영 관리할 수 있는 사람이 없어 개인정보 삭제 예정
정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차	데이터베이스가 왜 해킹되었는 지 궁금하며, 해킹을 방어할 수 있도록 노력할 예정

이해하기 쉬운 신고내용 #1

유출된 개인정보의 항목 및 규모	A 그룹: ID, 이름, 이메일, 휴대폰 번호 1,522건 B 그룹: 이름, 휴대폰 번호 88건 C 그룹: 이메일 365건
유출된 시점과 경위	**2025.05.17 11시35분** - 상위기관의 사이버안전센터에서 개인 메일 해킹으로 인한 자료 유출 확인 안내 메일 수신
유출피해 최소화 대책·조치 및 결과	**2025.05.17 13시00분** - 개인 메일과 사내 메일 패스워드 변경 및 2차 유출 방지를 위한 관련 메일 전량 삭제 **2025.05.17 13시15분** - 메일 계정 2차 비밀번호 인증 재점검 **2025.05.19 10시00분** - 개인정보보호책임자 주재로 전 직원 대상 개인 정보 처리 시 주의 사항 등 교육계획 수립 **2025.05.18 11시00분** - 안내된 전화번호로 피해 접수 등 상황 모니터링
정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차	핸드폰번호, 이메일 주소 등으로 스팸문자, 보이스피싱, 금융사기와 같은 2차 피해 방지를 위해 유출 대상 정보 주체에게 주의 안내 문자 발송 및 홈페이지 접속 시 패스워드 변경 조치 요청

이해하기 쉬운 신고내용 #2

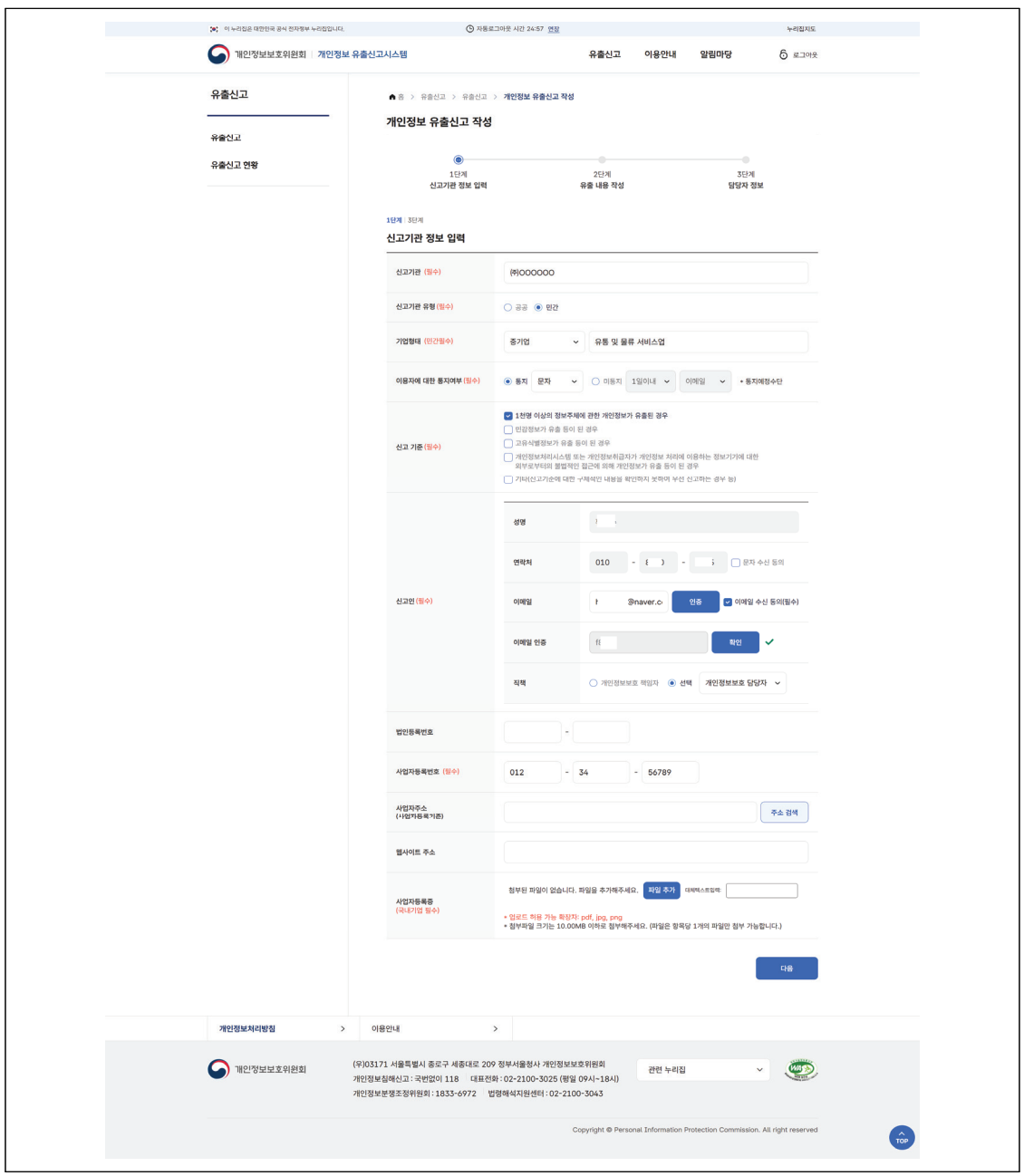
유출된 개인정보의 항목 및 규모	유출 규모: 100명 D 유출 항목: 이름, 성별, 휴대폰 번호 82명 E 유출 항목: 인종에 관한 민감정보 8명
유출된 시점과 경위	**1. 사고 발생 인지경위(인지시점)포함** - 2025.05.28 15:35 학부모가 G담당자에게 개인정보 유출 사실에 대한 내용을 사진 송부 **2. 유출된 시점 및 경위** - 2025.05.22 08:18 학생부 자료를 H담당자가 메신저를 통해 I담당자에게 전달 - 2025.05.28 08:28 I담당자는 학생부를 출력하여 게시판에 게시 - 2025.05.28 08:38 J학생이 학생부를 촬영하여 메신저를 통해 K, L, M, N에게 전달
유출피해 최소화 대책·조치 및 결과	- 2025.05.28. 16:35 학부모 대상 SMS 유출 통지 - 2025.05.28. 17:00 유출 항목, 일시 등 안내 - 2025.05.30. 14:00 재발방지 대책 수립
정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차	- 학부모 대상 N차 자료 유포 및 자료 방지 안내 - 피해 접수 담당 창구 운영 061-820-XXXX

신고 방법

- 개인정보 포털(www.privacy.go.kr)을 통하여 신고한다.

  ※ 메뉴 : 기업·공공서비스 〉 유출신고

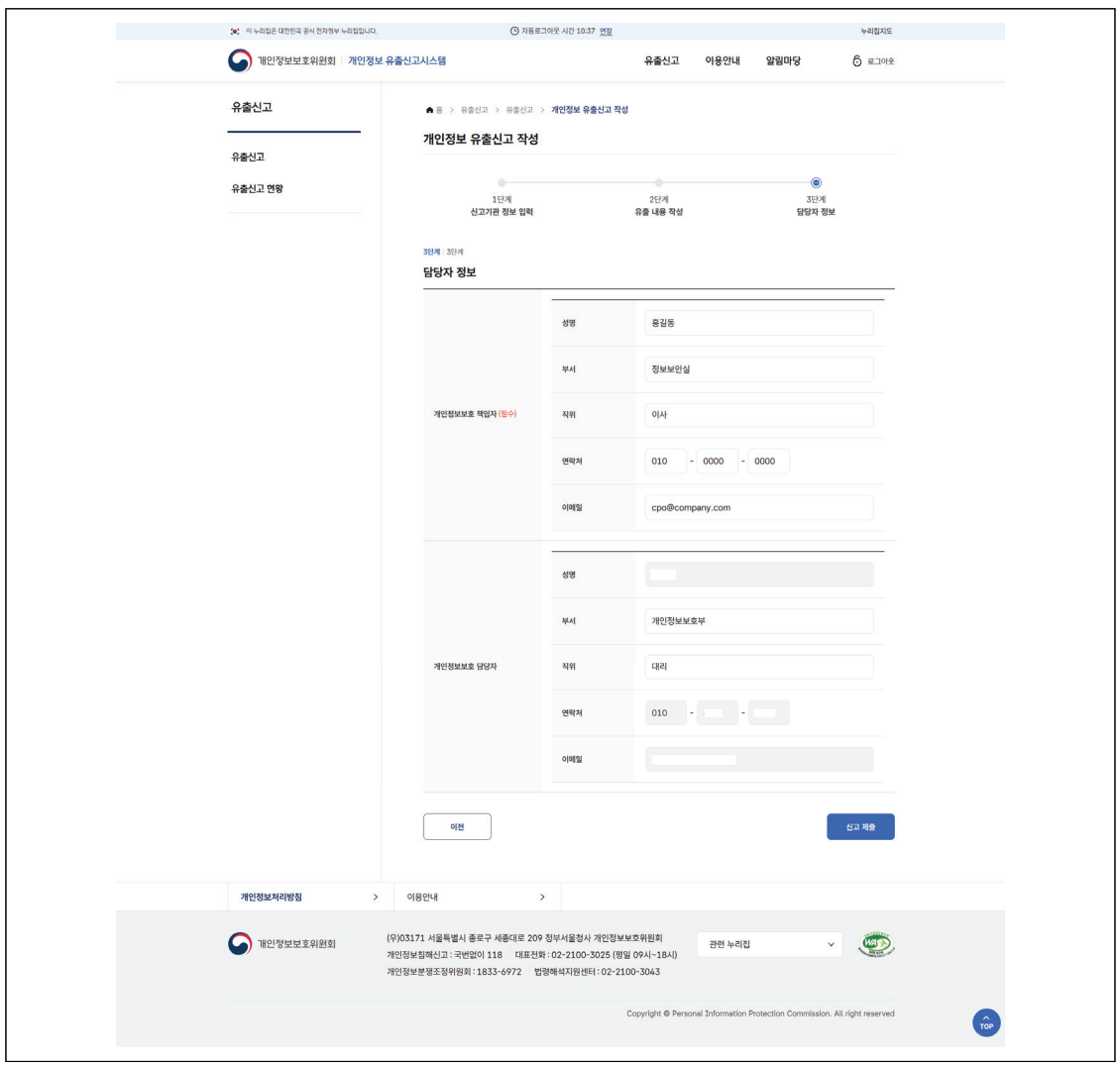
  - 개인정보 유출신고 시스템(brss.pipc.go.kr)에 직접 접속하여서도 신고 가능하다.



신고화면 1

이 누리집은 대한민국 공식 전자정부 누리집입니다.
자동로그아웃 시간 14:03 연장
누리집지도
개인정보보호위원회 | 개인정보 유출신고시스템
유출신고
이용안내
알림마당
로그아웃
유출신고
유출신고
유출신고 현황
홈 > 유출신고 > 유출신고 > 개인정보 유출신고 작성
개인정보 유출신고 작성
1단계
신고기관 정보 입력
2단계
유출 내용 작성
3단계
담당자 정보
2단계 | 3단계
유출 내용 작성
유출된 개인정보의 항목 및 규모
○ 항목: 아이디, 비밀번호, 이름, 휴대전화번호, 주소, 이메일주소, 계좌번호
○ 규모: 총 1,004건
- ID, PW, 이름, 휴대전화번호, 주소: 600건
- ID, PW, 이름, 휴대전화번호, 주소, 이메일주소, 계좌번호: 404건
138/4,000
유출된 시점과 그 경위
○ 유출 발생 시점: 2026-08-01 14:30
○ 유출 인지 시점: 2026-08-03 10:00
○ 유출 및 인지 경위
- [유출 경위] 물류관리 시스템(WMS)의 외부 연동 API 서버에 대한 외부의 비인가 접속(해킹 공격/SQL Injection)으로 인해 고객의 배송 정보 데이터베이스 일부가 외부로 유출됨
- [인지 경위] 2026년 8월 3일 10:00경 보안 모니터링 중 서버 관리자 계정의 이상 접근 로그 및 정보 유출 정황을 인지하여 분석을 진행함
266/4,000
유출피해 최소화 대책, 조치 및 결과 (필수)
○ 즉시 대응 조치
- [2026-08-03 10:30] 침입 경로로 확인된 외부 연동 API 서버 침입 차단 및 IP 접근 제한 조치 완료
- [2026-08-03 11:00] DB 관리자 비밀번호 변경 및 시스템 전반 취약점 점검 실시
○ 피해 최소화 조치
- [2026-08-03 18:30] 2차 피해 전담 상담 창구(CS 센터) 설치 및 전담 인력 배치 운영
- [2026-08-03 18:30~19:30] 유출 대상 고객 전원에게 개인정보 유출 사실 개별 통지(SMS 및 이메일 발송)
- 유출된 정보에 결제 비밀번호, 카드번호 등 금융 정보 및 주민등록번호는 포함되지 않음을 확인
344/4,000
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차 (필수)
○ 정보주체(고객) 행동 요령
- 본인 확인을 빙자한 출처가 불분명한 문자 메시지(SMS) 내 URL 링크 클릭 자제
- 당사 또는 택배사를 사칭한 스미싱/보이스피싱 전화 및 문자에 유의
- 회원 비밀번호 변경 권장 (동일한 ID/PW를 사용하는 타 사이트 비밀번호 포함)
○ 피해 발생 시 구제 절차 및 연락처
- 당사 개인정보 유출 전담 대응팀: 02-XXX-XXXX (평일 09:00~18:00)
- 당사 전용 이메일 문의: privacy@company.com
274/4,000
이전
다음
개인정보처리방침
이용안내
개인정보보호위원회
(우)03171 서울특별시 종로구 세종대로 209 정부서울청사 개인정보보호위원회
개인정보침해신고 : 국번없이 118 대표전화 : 02-2100-3025 (평일 09시~18시)
개인정보분쟁조정위원회 : 1833-6972 법령해석지원센터 : 02-2100-3043
관련 누리집
Copyright © Personal Information Protection Commission. All right reserved

신고화면 2


개인정보보호위원회 | 개인정보 유출신고시스템
유출신고
이용안내
알림마당
로그아웃
유출신고
유출신고
유출신고 현황
개인정보 유출신고 작성
1단계
신고기관 정보 입력
2단계
유출 내용 작성
3단계
담당자 정보
3단계 | 3단계
담당자 정보
개인정보보호 책임자 (필수)
성명
홍길동
부서
정보보안실
직위
이사
연락처
010 - 0000 - 0000
이메일
cpo@company.com
개인정보보호 담당자
성명
부서
개인정보보호부
직위
대리
연락처
010
이메일
이전
신고 제출
개인정보처리방침
이용안내
개인정보보호위원회
(우)03171 서울특별시 종로구 세종대로 209 정부서울청사 개인정보보호위원회
개인정보침해신고 : 국번없이 118 대표전화 : 02-2100-3025 (평일 09시~18시)
개인정보분쟁조정위원회 : 1833-6972 법령해석지원센터 : 02-2100-3043
관련 누리집
Copyright © Personal Information Protection Commission. All right reserved
TOP

신고화면 3

V

정보주체 피해 구제 및 재발 방지

V 정보주체 피해 구제 및 재발 방지

1 정보주체의 피해 구제

● 정보주체의 피해 구제 계획을 마련하고, 다음 제도를 안내해야 한다.

- 「개인정보 보호법」 제39조에 따른 손해배상 청구

> 정보주체가 개인정보처리자의 법 위반으로 인한 손해를 입증하면 고의 또는 과실을 입증하지 않고도 개인정보처리자에게 손해배상을 청구할 수 있다. 개인정보처리자의 고의 또는 중과실로 유출등이 발생한 경우 법원은 손해액의 5배를 넘지 않는 범위에서 손해배상액을 정할 수 있다(징벌적 손해배상)

- 「개인정보 보호법」 제39조의2에 따른 법정손해배상 청구

> 유출등의 손해액 입증이 곤란한 경우 정보주체는 실제 손해액 대신 300만 원 이하의 법정 손해배상액을 청구할 수 있다. 일반 손해배상과 선택적으로 청구할 수 있으며, 고의 또는 과실 및 손해액 입증 없이도 가능하다.

- 「개인정보 보호법」 제43조에 따른 개인정보 분쟁조정위원회 분쟁조정 신청

> 정보주체는 개인정보 분쟁조정위원회에 분쟁조정을 신청할 수 있다. 양 당사자가 조정안을 수락하면 재판상 화해와 동일한 효력을 가진다.

※ 개인정보 분쟁조정 신청(privacy.go.kr), 개인정보 분쟁조정위원회(www.kopico.go.kr / 국번 없이 1833-6972)

개인정보 분쟁조정위원회

개인정보 분쟁조정 신청

- 개인정보 유출등으로 인한 정보주체의 피해 신고·접수, 상담·문의 등 각종 민원 대응을 위한 방안을 마련한다.
  - 신속한 대응을 위해 상담 스크립트를 운영하고, 전화·이메일·홈페이지·SNS 등 다양한 채널을 통해 유출 사실 및 경위를 확인할 수 있는 창구를 마련한다.
  - 유출 규모와 상황을 종합적으로 고려하여 민원 대응 전담부서 운영, 통신회선 증설 등의 조치가 필요하다.

- 정보주체가 본인의 개인정보 유출등 여부를 확인할 수 있도록 별도의 홈페이지 등을 제공할 수 있다.
  - 본인확인 수단으로 핸드폰, 이메일 인증 등을 활용 가능하나, 법적 근거 없이 주민등록번호는 활용하지 않도록 주의한다.
  - 해당 홈페이지를 통하여 추가적인 개인정보 유출등이 발생하지 않도록 웹 취약점 제거, 전송구간 암호화 등 안전조치를 이행한다.

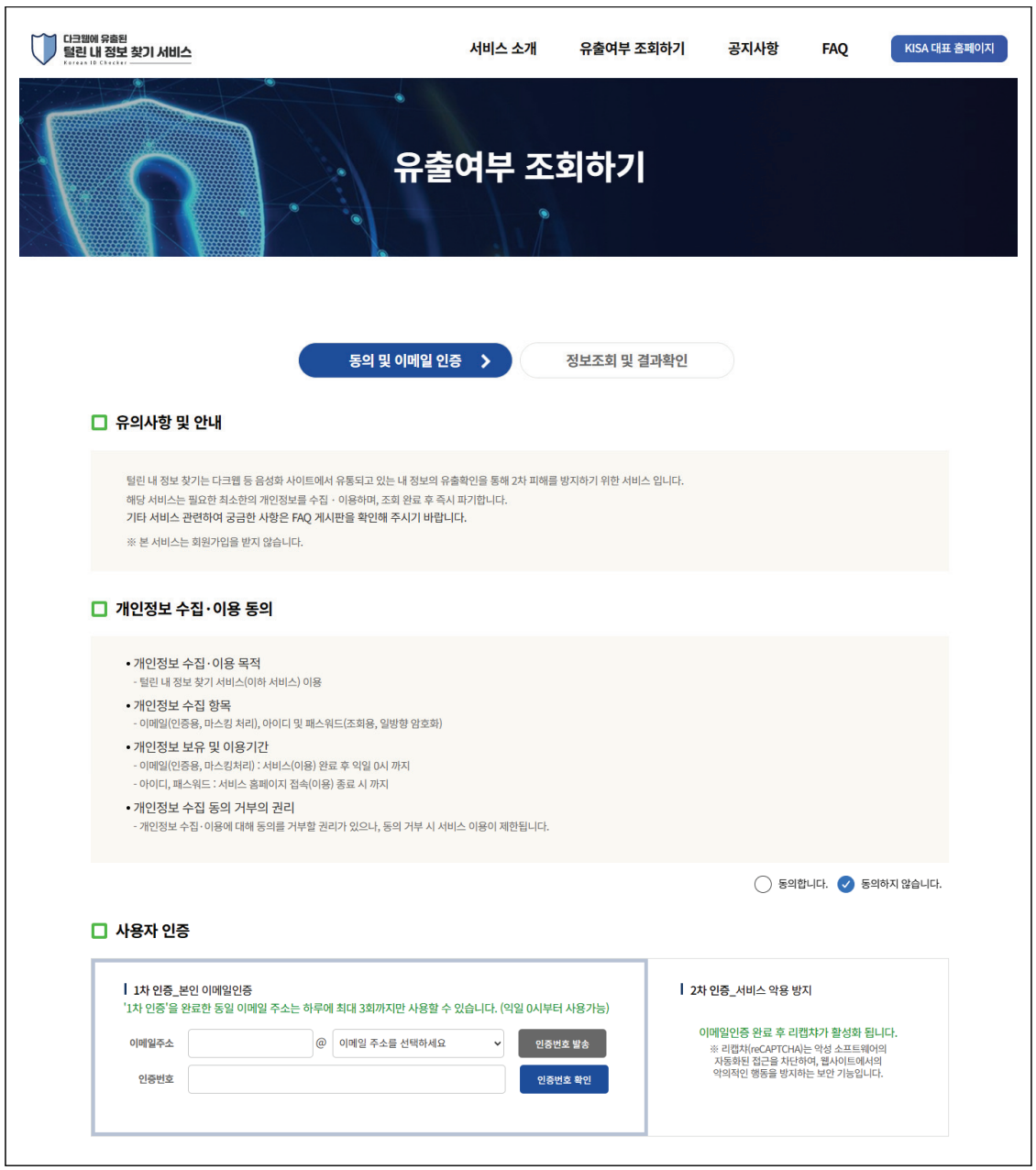
잘못 대응된 사례

• ○○사는 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 않은 경우
⇒ 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 한다.

- 유출등 대응 현장에서의 긴급·돌발 상황으로 인한 혼란을 최소화하기 위한 방안을 강구한다.
  - 현장에서 물리적 시스템 장애, 파괴, 또는 불필요한 인력 출입 등으로 인하여 개인정보가 분실·도난·훼손되지 않도록 주의한다.
- 보이스피싱 등 2차 피해 방지를 위한 유의사항을 사전 안내하고, 유출등·피해 및 대응 현황 등을 실시간으로 정확하고 투명하게 공개하여 고객 불안 해소를 위해 노력한다.

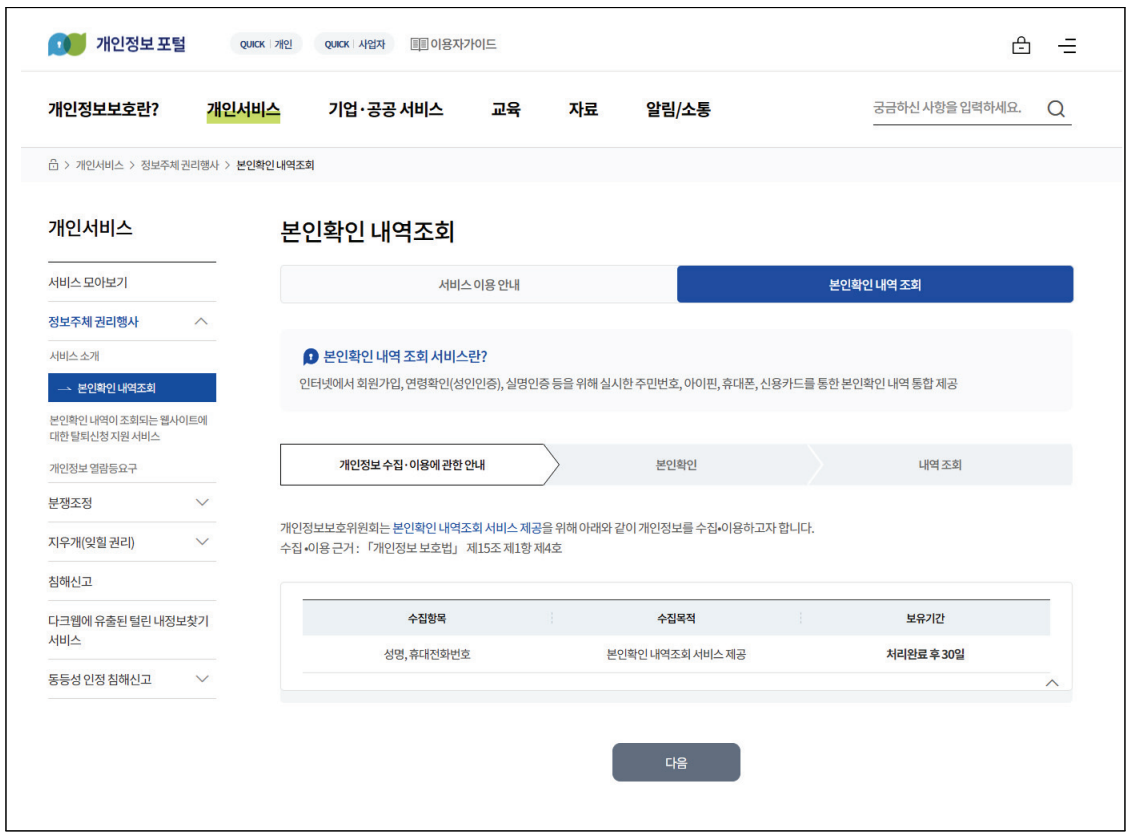
● 정보주체에게 안내할 수 있는 정부·공공 서비스는 다음과 같다.

- 다크웹 등에 유출된 본인 계정·비밀번호 조회 : 털린 내 정보 찾기(kidc.eprivacy.go.kr)



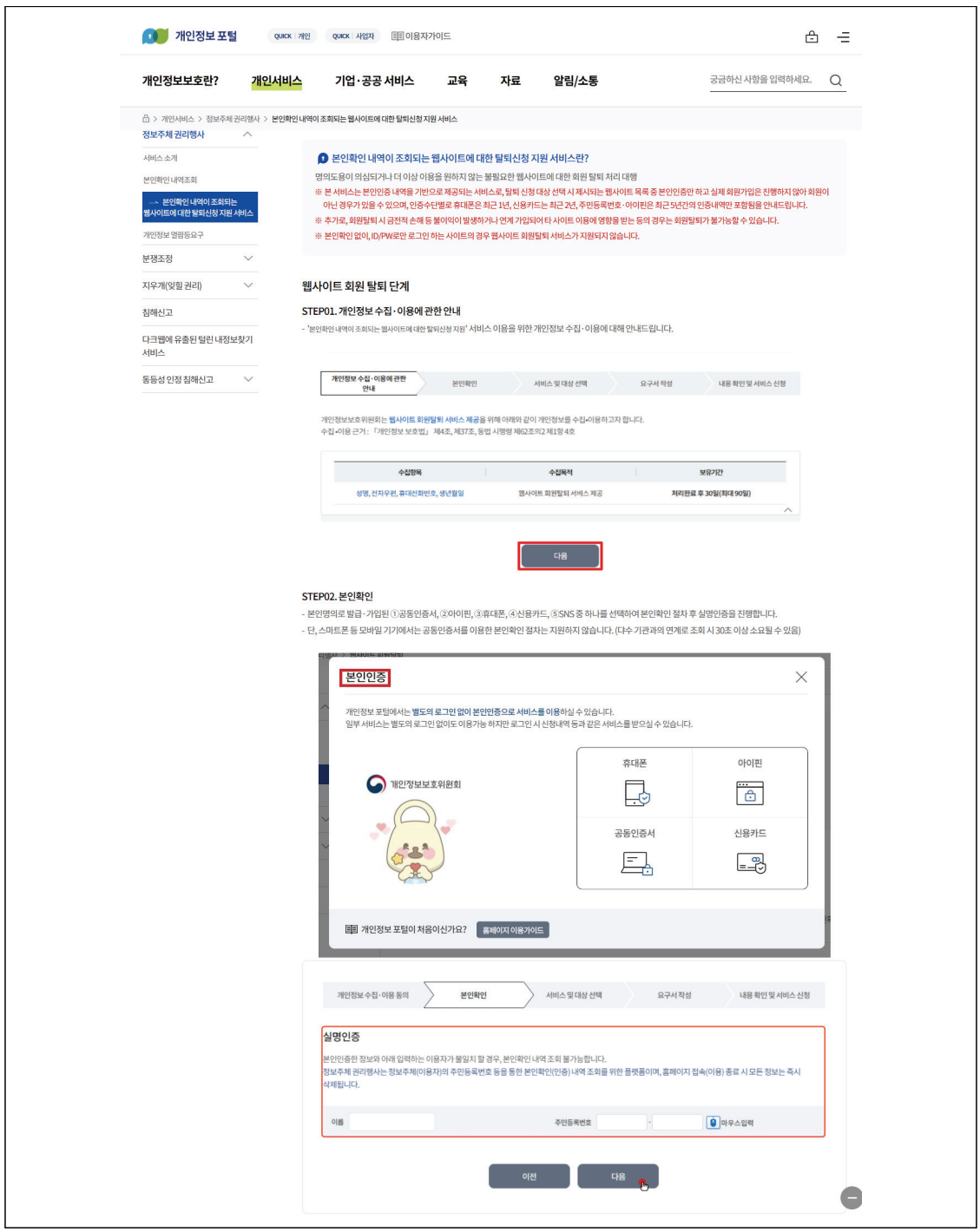
털린 내 정보 찾기

- 인터넷에서 회원가입, 연령확인(성인인증), 실명인증 등을 위해 실시한 주민번호, 아이핀, 휴대폰, 신용카드를 통한 본인확인 내역 통합 제공 : 본인확인 내역 조회(www.privacy.go.kr)



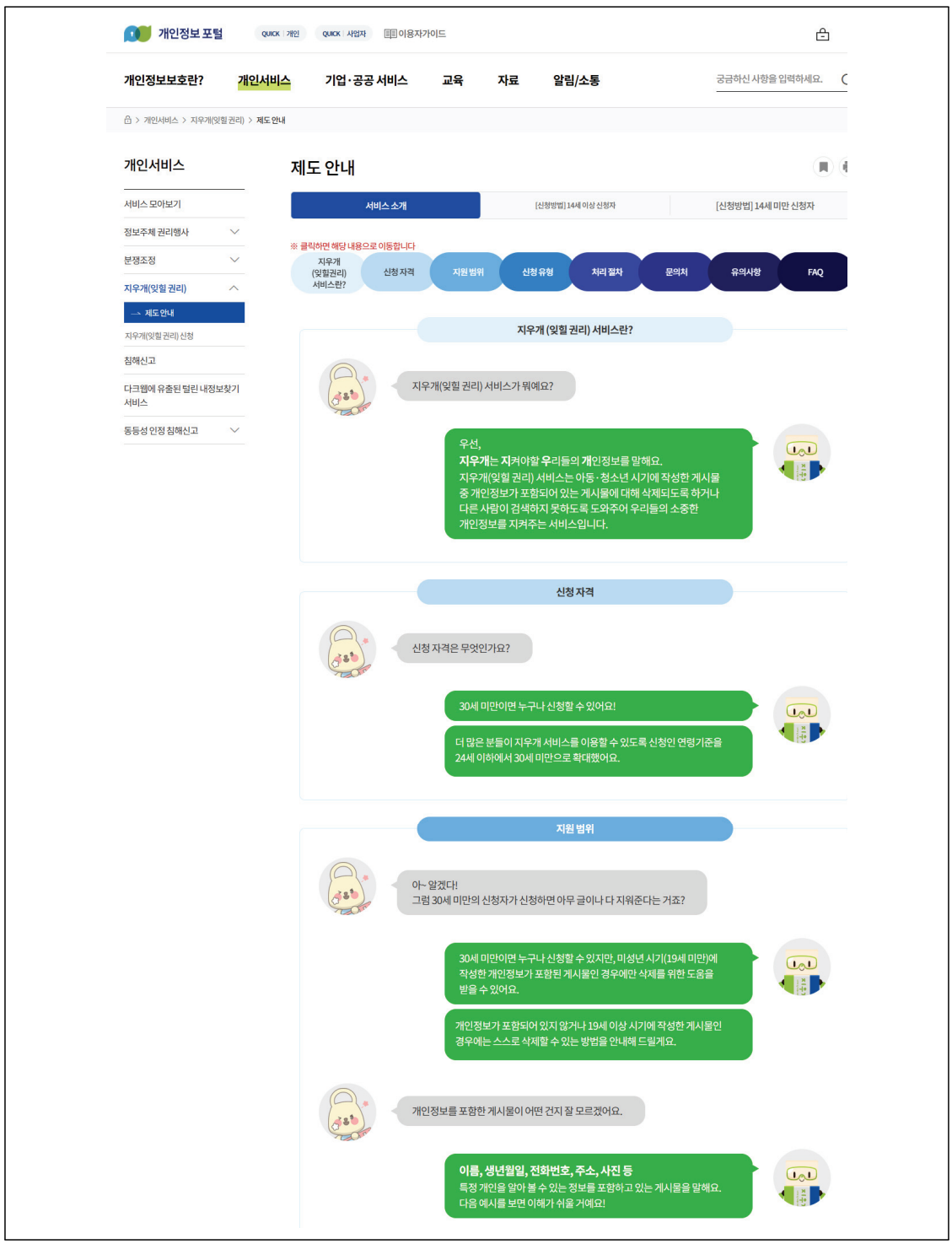
본인확인 내역 조회

- 본인확인 내역이 조회되는 웹사이트에 대한 탈퇴 신청 지원 : 본인확인 내역 조회 사이트 탈퇴 신청 (www.privacy.go.kr)



본인확인 내역 조회 사이트 탈퇴 신청

- 아동·청소년 시절 게시물 삭제 지원 : 지우개(잊힐 권리) 서비스(www.privacy.go.kr)



지우개(잊힐 권리) 서비스

2 재발 방지 대책 마련

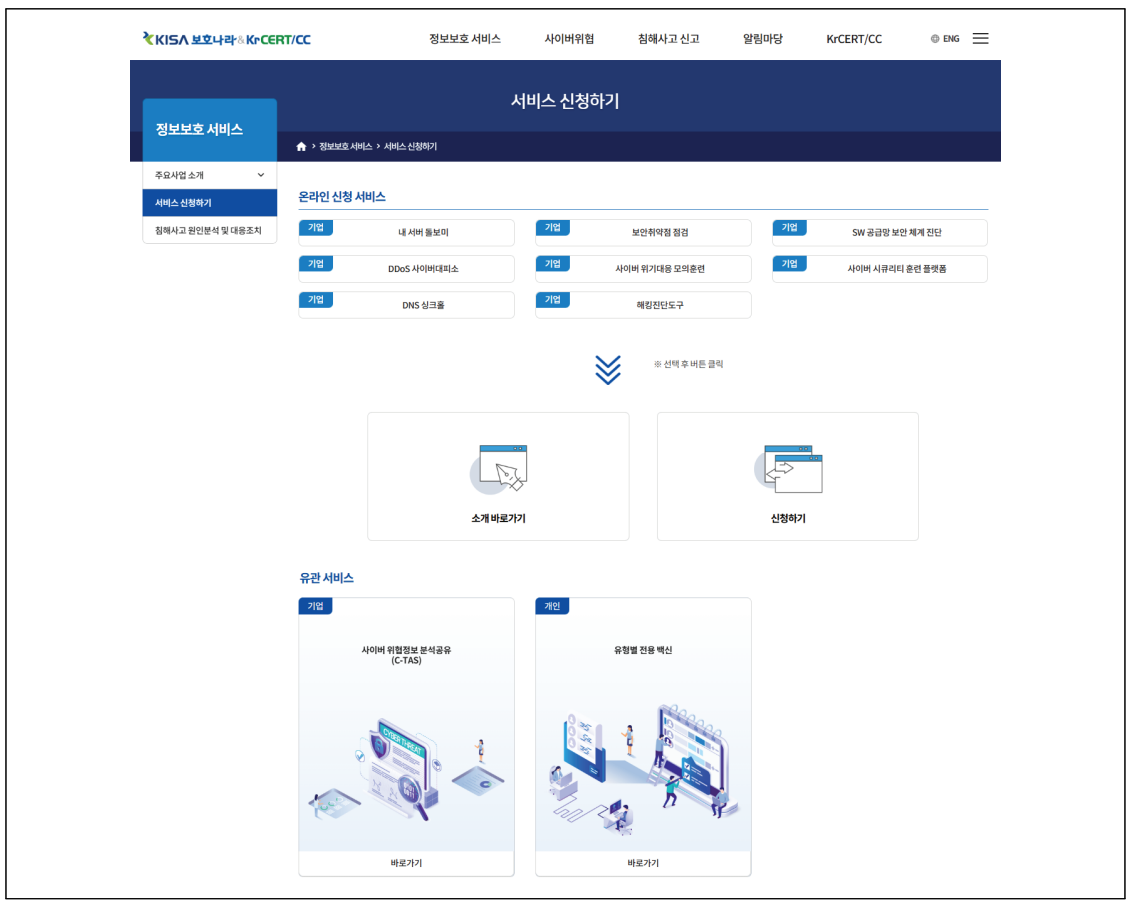
- 유출등의 원인, 취약점 등을 명확히 분석하고, 그에 따른 구체적인 재발 방지 대책을 수립한다.
  - 원인 분석 결과는 기술적·관리적·물리적 측면을 모두 포함한다.
  - 수립된 대책은 책임자(CPO 등)의 결재를 거쳐 공식 문서로 남긴다.
- 유출등 원인과 유출등 경로 등을 고려하여 안전성 확보 조치를 재점검하고 강화한다.
  - 접근권한 관리, 접근통제, 암호화, 접속기록 보관·점검, 악성코드 방지, 백업·복구 등 기술적 조치를 보완한다.

안전성 확보 조치 강화 예시

- 홈페이지의 취약점을 연 1회 이상 정기적으로 점검
- 개인정보가 인터넷상에 노출되는 것을 방지하기 위해 인증 절차 추가 및 로봇 배제 규칙을 적용하여 홈페이지 접근을 제한
- 홈페이지에 첨부파일을 포함한 게시글 작성 시 개인정보 포함 여부를 확인
- 홈페이지 게시판 등에 정보주체가 글 작성 시 개인정보가 노출되지 않도록 주의할 것을 안내
- 관리자 페이지에 접근하는 IP를 제한하거나 아이디, 비밀번호 외 추가적인 인증수단을 사용하여 접속

  - 개인정보 유출등 대응 시나리오 작성, 정기 취약점 점검 및 모의해킹, 모의훈련 등을 정례화하는 등 유출등 대응체계를 점검하고, 점검 결과에 따른 개선 조치를 이행하는 등 지속적으로 보완한다.

    ※ 중소기업의 경우 한국인터넷진흥원(KISA)에서 제공하는 보안 취약점 점검 서비스(boho.or.kr)를 이용할 수 있다.



보안 취약점 점검 서비스

- 임직원·개인정보취급자를 대상으로 개인정보보호 교육을 실시하고 보안인식을 제고한다.
  - 유출등 발생 즉시 교육을 실시하고, 사례를 공유하여 동일·유사 사고 재발을 방지한다.
  - 연 1회 이상 정기 개인정보보호 교육을 실시한다.
  - 개인정보취급자에 대해서는 직무별 맞춤 교육을 추가로 실시한다.
- 개인정보 처리 업무를 위탁한 경우 수탁자 및 관계사의 안전조치 이행 여부를 점검하고 관리·감독을 강화한다.
  - 수탁자의 개인정보 처리 현황 및 안전조치 이행 상태를 정기적으로 점검한다.
  - 수탁계약서에 개인정보보호 의무사항을 명시하고, 위반 시 책임 소재를 명확히 한다.
- 수립된 재발 방지 대책의 이행 상태를 정기적으로 점검하고, 결과를 책임자(CPO 등)에게 보고한다.
  - 개인정보보호위원회 등 감독기관의 시정명령이 있는 경우 이행 결과를 기한 내에 보고한다.
  - 이행 점검 결과는 행정조사·감사 대비 자료로 활용될 수 있도록 기록·보관한다.

부록

부록 1 개인신용정보 누설 통지·신고

■ 통지 의무

- 신용정보회사등은 개인신용정보가 누설되었음을 알게 되었을 때에는 「개인정보 보호법」 제34조제1항 각 호의 사항을 정보주체에게 통지하여야 한다.
- 1만 명 이상의 개인신용정보가 누설된 경우에는 개별 통지와 별도로 아래의 어느 하나에 해당하는 방법으로 알려야 한다.
  - 인터넷 홈페이지 게시 : 15일
  - 사무실이나 점포 등에서의 당사자 열람 : 15일
  - 일간지 등 게재 : 7일

■ 신고 의무

- 신용정보회사등은 1만 명 이상의 개인신용정보가 누설된 경우 아래 구분에 따라 소관 기관에 신고해야 한다.

구분	신고 기관
상거래기업 및 법인	개인정보보호위원회 또는 한국인터넷진흥원(KISA)
신용정보회사등 (상거래기업 및 법인 제외)	금융위원회 또는 금융감독원

<table>
<tr><th colspan="2">근거 법률</th><th>개인정보 보호법
제34조(개인정보 유출등의 통지·신고)</th><th>신용정보법
제39조의4(개인신용정보 누설통지 등)</th></tr>
<tr><td colspan="2">적용 대상</td><td>개인정보처리자</td><td>신용정보회사등</td></tr>
<tr><td colspan="2">적용 범위</td><td>개인정보의 유출등</td><td>개인신용정보 누설</td></tr>
<tr><td rowspan="4">통지</td><td>규모</td><td colspan="2">1명 이상</td></tr>
<tr><td>시점</td><td>72시간 내</td><td>72시간 내(권고)</td></tr>
<tr><td rowspan="2">방법</td><td colspan="2">개별 통지(문자메시지, 이메일, 전화, 서면 등)</td></tr>
<tr><td>다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우, 인터넷 홈페이지에 30일 이상 게시로 갈음
홈페이지를 운영하지 아니하는 경우, 사업장 등의 보기 쉬운 장소에 30일 이상 게시로 갈음</td><td>다만, 1만명 이상의 개인신용정보가 누설된 경우, 개별 통지 외에 인터넷 홈페이지에 게시(15일), 사무실 등에서 당사자가 열람(15일) 또는 일간지 등에 게재(7일)</td></tr>
<tr><td>항목</td><td colspan="2">• 유출등이 된 개인정보 항목, 유출등이 된 시점과 그 경위, 정보주체가 할 수 있는 피해 최소화 조치, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처, 정보주체의 법적 권리와 그 행사 방법</td></tr>
<tr><td rowspan="4">신고</td><td>규모</td><td>1. 1천명 이상 유출등
2. 민감정보, 고유식별정보 유출등
3. 외부로부터의 불법적인 접근에 의해 개인정보가 유출등</td><td>1만명 이상 개인신용정보 누설</td></tr>
<tr><td>시점</td><td>72시간 이내</td><td>72시간 이내(권고)</td></tr>
<tr><td rowspan="2">기관</td><td rowspan="2">개인정보보호위원회 등</td><td>상거래기업 및 법인 : 개인정보보호위원회 등</td></tr>
<tr><td>신용정보회사등(상거래기업 및 법인 제외) : 금융위원회 등</td></tr>
<tr><td colspan="2">벌칙 규정</td><td colspan="2">3천만원 이하의 과태료</td></tr>
</table>

신용정보법

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.

신용정보법 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 보급 지역으로 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.

신용정보업 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 유출등 신고서 양식

「(개인정보보호위원회) 표준 개인정보 보호지침」 [별지 제1호서식]

개인정보 유출등 신고서

<table>
<tr><td>기관명</td><td colspan="5"></td></tr>
<tr><td>유출등이 된 개인정보 항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출등이 된 시점과 그 경위</td><td colspan="5"></td></tr>
<tr><td>유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등</td><td colspan="5"></td></tr>
<tr><td>개인정보처리자의 대응조치 및 피해 구제 절차</td><td colspan="5"></td></tr>
<tr><td>정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처</td><td colspan="5"></td></tr>
<tr><td rowspan="3">유출등 신고 담당자</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보 보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>담당자</td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td rowspan="2">유출등 신고접수기관</td><td>기관명</td><td>담당자명</td><td>연락처</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

부록 3 침해사고 신고 및 경찰 수사

침해사고 신고

- 해킹 등 침해사고가 발생하면 「개인정보 보호법」에 따른 유출등의 신고와 별도로 즉시 관계 기관에 신고하여 사고 원인분석 및 취약점 보완조치 등을 실시한다.
  - 공공부문 : 국가정보원
  - 민간부문(정보통신서비스 제공자) : 과학기술정보통신부 또는 한국인터넷진흥원(보호나라, boho.or.kr)

※ 법적 근거 : 「정보통신망법 이용촉진 및 정보보호 등에 관한 법률」 제48조의3에 따라 침해사고 인지 후 24시간 이내 신고 의무

※ 침해사고 신고 : KISA 보호나라 → 침해사고 신고 → 신고하기, ☎ 국번 없이 118

침해사고 신고 안내

이용방법

자주묻는 질문 FAQ

과학기술정보통신부와 한국인터넷진흥원은 아래와 같이 『정보통신망 이용 촉진 및 정보보호 등에 관한 법률』(이하, 정보통신망법)에 근거하여 민간분야 인터넷 침해사고 예방 및 대응 활동을 수행하고 있습니다.

☞ 제 48조의3(침해사고의 신고 등) : 정보통신서비스 제공자의 침해사고 신고 접수
※ 침해사고 신고는 동법 시행령 제58조의2(침해사고 신고의 시기, 방법 및 절차 등)에 근거하여 침해사고의 발생을 알게 된 때부터 24시간 이내에 신고
※ 침해사고의 발생을 알게 된 때부터 24시간 이후에 신고하거나 신고를 아니할 시, 동법 제76조(과태료)에 근거하여 3천만원 이하의 과태료 부과

☞ 제 48조의4(침해사고의 원인 분석 등) : 정보통신서비스 제공자의 침해사고 관련 자료 보전 및 제출 요구, 현장조사 등
※ 침해사고 관련 자료 보전 명령을 위반할 시, 동법 제73조(벌칙)에 근거하여 2년 이하의 징역 또는 2천만원 이하의 벌금 부과
※ 침해사고 관련 자료를 제출하지 아니하거나 거짓으로 제출할 시, 동법 제76조(과태료)에 근거하여 1천만원 이하의 과태료 부과

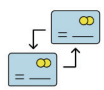
정보통신서비스 제공자는 침해사고 발생 즉시 정보통신망법 48조의3(침해사고의 신고 등)에 따라 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 하며, 제48조의4(침해사고의 원인 분석 등)침해사고의 원인분석 및 그에 따라 피해의 확산 방지를 위하여 사고 대응, 복구 및 재발방지에 필요한 조치를 하여야 합니다.

경찰 수사

- 해킹·내부자 유출등 범죄 혐의가 의심되는 경우, 해커 등 개인정보 유출자 검거 및 개인정보 회수를 위한 조치가 필요한 경우에는 개인정보의 유출등 신고, 침해사고 신고와 별도로 경찰청에 범인 검거를 위한 형사고소·고발 또는 수사를 요청하고 유출등이 된 개인정보 회수를 위한 조치를 실시
  - 관할 경찰서 또는 경찰청 사이버범죄 신고시스템(ECRM, ecrm.police.go.kr)을 통해 진행 가능

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

부록 4 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 신규가입 시 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)
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자 메시지에 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, 불법스팸신고(☎118)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	정보주체 대응 방안
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, 불법스팸신고(☎118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름, 이메일, 연락처만으로 회원 가입 가능 ② 명의도용을 통해 본인도 모르는 수십여 개의 웹사이트 가입하여 개인정보 불법 이용	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸신고(☎118) ※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가
	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, 연소득 등 활용 대출 스팸 발송, 자동차 보유 여부를 활용한 보험 스팸 발송 등 특정 유형의 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, 불법스팸신고(☎118) ※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스
	사회공학적 기법을 활용한 악성코드 유포메일 발송	이메일 주소 등	① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도하는 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 최신 버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸신고(☎118)

개인정보 유출등 대응 안내서

발 행 일 2026년 9월
발 행 처 개인정보보호위원회
지원기관 한국인터넷진흥원
디 자 인 (사)아름다운사람들(☎02-6948-9650)

※ 최신자료는 “개인정보보호위원회 누리집(pipc.go.kr)”, “개인정보 포털(privacy.go.kr)”에서 확인할 수 있습니다.

개인정보 유출등 대응 안내서

개인정보보호위원회
Personal Information Protection Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY