(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0085618
(43) 공개일자 2025년06월12일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 16/951* (2019.01)
G06F 16/955 (2019.01)
(52) CPC특허분류
G06F 21/6245 (2013.01)
G06F 16/951 (2019.01)
(21) 출원번호 10-2024-0174475
(22) 출원일자 2024년11월29일
심사청구일자 2024년11월29일
(30) 우선권주장
1020230173950 2023년12월05일 대한민국(KR)

(71) 출원인
주식회사 오내피플
서울특별시 마포구 마포대로 122, 1703호 (공덕동, 프론트원)
(72) 발명자
조아영
서울 마포구 백범로31길 21 서울창업허브 본관 631호
(74) 대리인
특허법인비엘티

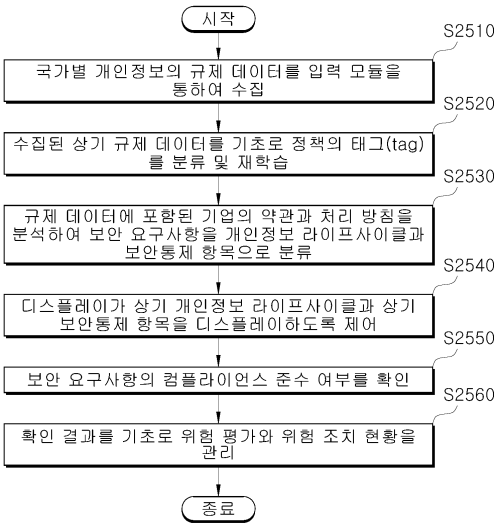
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **컴플라이언스 요구사항 분석 및 점검 자동화 장치 및 그 제어 방법**

(57) 요 약

본본 개시는 컴플라이언스 요구 사항 분석 및 점검 자동화 장치 및 그 제어 방법에 관한 것으로, 국가별 개인정보의 규제 데이터를 입력 모듈을 통하여 수집하고, 수집된 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습하고, 상기 규제 데이터에 포함된 기업의 계약, 약관, 정책, 지침 및 개인정보 처리방침 중 적어도 하나를 분석하여 상기 기업의 보안 요구사항을 개인정보 라이프사이클 및 보안통제 항목으로 분류하고, 상기 보안 요구사항의 컴플라이언스 준수 여부를 확인하고, 확인 결과를 기초로 위험 평가와 위험 조치 현황을 관리하는 것을 그 요지로 한다.

대 표 도 - 도25



(52) CPC특허분류
G06F 16/955 (2019.01)
G06F 21/6227 (2013.01)

명 세 서

청구범위

청구항 1

국가별 개인정보의 규제 데이터를 수집하는 입력 모듈;

모바일 디바이스를 포함하는 외부 장치 및 상기 규제 데이터를 송수신하는 통신 모듈;

컴플라이언스 요구사항 분석 및 점검 자동화 동작의 수행을 위한 적어도 하나의 프로세스가 저장되고, 규제 준수 관리자의 입력 및 데이터를 저장하는 메모리; 및

상기 프로세스에 따라 동작을 수행하는 프로세서를 포함하되,

상기 프로세서는,

상기 입력 모듈을 통해 수집되는 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습하고,

상기 규제 데이터에 포함된 기업의 계약, 약관, 정책, 지침 및 개인정보 처리방침 중 적어도 하나를 분석하여 상기 기업의 보안 요구사항을 개인정보 라이프사이클 및 보안통제 항목으로 분류하고,

상기 보안 요구사항의 컴플라이언스 준수 여부를 확인하고,

상기 확인된 결과를 기초로 위험 평가 및 위험 조치 현황을 관리하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 2

제 1 항에 있어서, 상기 프로세서는,

상기 규제 데이터의 크롤링, 업로드 및 링크 등록, 및 입력 중 적어도 하나를 수행하고,

상기 규제 데이터의 조항별 주요 키워드를 도출하여 개인정보 규제의 태그(tag)를 부여하고,

상기 태그 내용의 유사도를 계산하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 3

제 2 항에 있어서, 상기 프로세서는,

상기 규제 데이터의 업데이트가 발생하면, 상기 업데이트된 규제 데이터에 대한 태그를 부여하고,

상기 업데이트된 규제 데이터 내의 업데이트된 조항과 기존 조항의 유사도를 계산하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 4

제 1 항에 있어서, 상기 프로세서는,

국가별로 개인정보 보호 규제를 조사하고,

상기 조사한 개인정보 보호 규제를 마이크로 규제 또는 공통 규제로 분류하는, 컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 5

제 1 항에 있어서, 상기 프로세서는,

상기 보안 요구사항과 기 분석된 보안 위험도에 대한 결과값을 매핑하고,

상기 결과값과 상기 보안 요구사항의 기준값을 비교하고,

상기 결과값이 상기 기준값 이상인 경우, 컴플라이언스를 준수했거나 또는 확인이 필요한 사항으로 분류하고,

상기 결과값이 상기 기준값 미만인 경우, 컴플라이언스를 준수하지 않거나 또는 확인이 필요한 사항으로 분류하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 6

제 5 항에 있어서, 상기 프로세서는,

상기 확인이 필요한 사항인 경우, 다른 모듈의 결과값을 매핑하여 계산하거나 입력값을 상기 규제 준수 관리자로부터 수신하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 7

제 1 항에 있어서, 상기 프로세서는,

상기 보안 요구사항과 기 분석된 보안 위험도에 대한 결과값을 매핑하고,

상기 매핑된 결과를 기초로 위험도를 계산하고,

상기 위험도는 과태료 가능성, 규제위반 위험성 및 개인정보 유출위험성 중 적어도 하나를 포함하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 8

제 7 항에 있어서, 상기 프로세서는,

상기 위험도에 대응하는 위험 조치를 수행하는 담당자, 기한, 우선순위, 및 위험 수준을 수신하고,

위험 조치 사항을 포함하는 메시지를 상기 규제 준수 관리자의 디바이스로 전송하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 9

제 8 항에 있어서, 상기 프로세서는,

위험 조치 트리거가 발생하면, 상태를 위험 조치 완료로 변경하여 위험 수준을 관리하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 장치.

청구항 10

장치의 프로세서가 수행하는, 컴플라이언스 요구 사항 분석 및 점검 자동화 방법에 있어서,

국가별 개인정보의 규제 데이터를 수집하는 단계;

수집된 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습하는 단계;

상기 규제 데이터에 포함된 기업의 계약, 약관, 정책, 지침 및 개인정보 처리방침 중 적어도 하나를 분석하여 상기 기업의 보안 요구사항을 개인정보 라이프사이클 및 보안통제 항목으로 분류하는 단계;

상기 보안 요구사항의 컴플라이언스 준수 여부를 확인하는 단계; 및

확인 결과를 기초로 위험 평가와 위험 조치 현황을 관리하는 단계를 포함하는,

컴플라이언스 요구 사항 분석 및 점검 자동화 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 분석 및 점검 자동화 장치에 관한 것이다. 보다 상세하게는, 컴플라이언스 요구사항 분석 및 점검 자동화 장치 및 그 제어 방법에 관한 것이다.

배 경 기 술

[0002] 최근 많은 기업, 기관들이 본점을 국내에 두고 해외 거주 고객을 위한 서비스를 제공하는 글로벌 네트워크 또는 글로벌 지점(이하, 글로벌 네트워크로 통칭함)을 운영하고 있다. 그러나 현실적으로 글로벌 네트워크에서 발생하는 각종 정보보호 규제에 대응하는데 있어 한계점이 존재한다. 국내에서는 정보보호 담당자가 존재하고 해당 정보보호 규제의 변화 내용을 파악하고, 그에 기초하여 정보보호 관리 체계를 수립하여 대응할 수 있다.

[0003] 하지만, 본점 집중으로 글로벌 정보보호를 관리 운영하는 국외 지점의 경우, 국가별 법률 체계의 차이, 현지 근무 직원의 정보보호 규제에 대한 이해, 정보보호 기술 대응의 한계 등으로 인하여 규제 대응에 미흡함이 존재하고, 이로 인한 정보보호 수준의 질적 저하로 인하여 장기적으로는 정보보호 규제 대응 실패, 정보보호 저하 등의 문제점이 야기된다.

[0004] 이러한 문제점을 해결하기 위해 글로벌 네트워크에서는 글로벌 정보보호 담당자를 지정하여 정보보호 규제 대응과 정보보호 운영 등의 절차를 수행하고 있다.

[0005] 그런데 종래 기술의 경우, 글로벌 정보보호 담당자조차도 규제 변화의 관리, 정보보호 모니터링, 본국 수준의 정보보호 수준 관리에는 한계를 가지므로, 정보보호 누수 현상의 발생을 초래할 수 있는 문제를 갖고 있다.

[0006] 또한 종래 기술의 경우, 이를 위한 해결 방안으로 네트워크 장비를 이용하여국가별 규제 대응 컨설팅 수행 등을 수행하고는 있으나, 글로벌 정보보호 규제 컨설팅 조차도 통일된 정보보호 규제 관리 방법론 부재와 정보보호 규제 내용, 각종 감사 자료 등 산출물 유지 관리에는 어려움이 있어서 사용자가 불편함을 느끼는 문제점이 있었다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 미국 공개특허공보 US2023/0047653 A1, (공개일: 2023.02.16.)

발명의 내용

해결하려는 과제

[0008] 본 개시에 개시된 실시 예는 국가별 개인정보 규제를 수집하고 정책의 태그를 자동분류 및 재학습하는 컴플라이언스 요구사항 분석 및 점검 자동화 장치를 제공하는 것을 목적으로 한다.

[0009] 본 개시에 개시된 실시 예는 기업의 약관과 처리 방침을 분석하여 보안요구사항을 개인정보 라이프사이클과 보안통제 항목으로 분류하며 화면에 디스플레이하는 컴플라이언스 요구사항 분석 및 점검 자동화 장치를 제공하는 것을 목적으로 한다.

[0010] 본 개시에 개시된 실시 예는 컴플라이언스 준수 여부를 자동으로 점검하고, 점검 결과를 바탕으로 위험 평가와 위험 조치 현황을 관리하는 컴플라이언스 요구사항 분석 및 점검 자동화 장치를 제공하는 것을 목적으로 한다.

[0011] 본 개시가 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 본 개시에 따른 컴플라이언스 요구사항 분석 및 점검 자동화 장치는, 국가별 개인정보의 규제 데이터를 수집하는 입력 모듈; 모바일 디바이스를 포함하는 외부 장치 및 상기 규제 데이터를 송수신하는 통신 모듈; 컴플라이언스 요구사항 분석 및 점검 자동화 동작의 수행을 위한 적어도 하나의 프로세스가 저장되고, 규제 준수 관리자의 입력 및 데이터를 저장하는 메모리; 및 상기 프로세스에 따라 동작을 수행하는 프로세서를 포함하되, 상기

프로세서는, 상기 입력 모듈을 통해 수집되는 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습하고, 상기 규제 데이터에 포함된 기업의 계약, 약관, 정책, 지침 및 개인정보 처리방침 중 적어도 하나를 분석하여 상기 기업의 보안 요구사항을 개인정보 라이프사이클 및 보안통제 항목으로 분류하고, 상기 보안 요구사항의 컴플라이언스 준수 여부를 확인하고, 상기 확인된 결과를 기초로 위험 평가 및 위험 조치 현황을 관리할 수 있다.

[0013] 이때, 상기 프로세서는 상기 규제 데이터의 크롤링, 업로드 및 링크 등록, 및 입력 중 적어도 하나를 수행하고, 상기 규제 데이터의 조항별 주요 키워드를 도출하여 개인정보 규제의 태그(tag)를 부여하고, 상기 태그 내용의 유사도를 계산할 수 있다.

[0014] 또한, 상기 프로세서는 상기 규제 데이터의 업데이트가 발생하면, 상기 업데이트된 규제 데이터에 대한 태그를 부여하고, 상기 업데이트된 규제 데이터 내의 업데이트된 조항과 기존 조항의 유사도를 계산할 수 있다.

[0015] 또한, 상기 프로세서는 국가별로 개인정보 보호 규제를 조사하고, 상기 조사한 개인정보 보호 규제를 마이크로 규제 또는 공통 규제로 분류할 수 있다.

[0016] 또한, 상기 프로세서는 상기 보안 요구사항과 기 분석된 보안 위험도에 대한 결과값을 매핑하고, 상기 결과값과 상기 보안 요구사항의 기준값을 비교하고, 상기 결과값이 상기 기준값 이상인 경우, 컴플라이언스를 준수했거나 또는 확인이 필요한 사항으로 분류하고, 상기 결과값이 상기 기준값 미만인 경우, 컴플라이언스를 준수하지 않거나 또는 확인이 필요한 사항으로 분류할 수 있다.

[0017] 또한, 상기 프로세서는 상기 확인이 필요한 사항인 경우, 다른 모듈의 결과값을 매핑하여 계산하거나 입력값을 상기 규제 준수 관리자로부터 수신할 수 있다.

[0018] 또한, 상기 프로세서는 상기 보안 요구사항과 기 분석된 보안 위험도에 대한 결과값을 매핑하고, 상기 매핑된 결과를 기초로 위험도를 계산하고, 상기 위험도는 과태료 가능성, 규제위반 위험성 및 개인정보 유출위험성 중 적어도 하나를 포함할 수 있다.

[0019] 또한, 상기 프로세서는 상기 위험도에 대응하는 위험 조치를 수행하는 담당자, 기한, 우선순위, 및 위험 수준을 수신하고, 위험 조치 사항을 포함하는 메시지를 상기 규제 준수 관리자의 디바이스로 전송할 수 있다.

[0020] 이때, 상기 프로세서는 위험 조치 트리거가 발생하면, 상태를 위험 조치 완료로 변경하여 위험 수준을 관리할 수 있다.

[0021] 또한, 본 개시에 따른 장치의 프로세서가 수행하는 컴플라이언스 요구 사항 분석 및 점검 자동화 방법은, 국가별 개인정보의 규제 데이터를 수집하는 단계; 수집된 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습하는 단계; 상기 규제 데이터에 포함된 기업의 계약, 약관, 정책, 지침 및 개인정보 처리방침 중 적어도 하나를 분석하여 상기 기업의 보안 요구사항을 개인정보 라이프사이클 및 보안통제 항목으로 분류하는 단계; 상기 보안 요구사항의 컴플라이언스 준수 여부를 확인하는 단계; 및 확인 결과를 기초로 위험 평가와 위험 조치 현황을 관리하는 단계를 포함할 수 있다.

[0022] 이 외에도, 본 개시를 구현하기 위한 방법을 실행하기 위해 컴퓨터 판독 가능한 기록 매체에 저장된 컴퓨터 프로그램이 더 제공될 수 있다.

[0023] 이 외에도, 본 개시를 구현하기 위한 방법을 실행하기 위한 컴퓨터 프로그램을 기록하는 컴퓨터 판독 가능한 기록 매체가 더 제공될 수 있다.

발명의 효과

[0024] 본 발명에 따르면, 국가별 개인정보 규제를 수집하고 정책의 태그를 자동분류 및 재학습할 수 있으므로 사용자 편의성을 향상 시킬 수 있다.

[0025] 본 발명에 따르면, 기업의 약관과 처리 방침을 분석하여 보안요구사항을 개인정보 라이프사이클과 보안통제 항목으로 분류하며 화면에 디스플레이할 수 있으므로 사용자 편의성을 향상 시킬 수 있다.

[0026] 본 발명에 따르면, 컴플라이언스 준수 여부를 자동으로 점검하고, 점검 결과를 바탕으로 위험 평가와 위험 조치 현황을 관리할 수 있으므로 사용자 편의성을 향상 시킬 수 있다.

[0027] 본 개시의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로

부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0028] 도 1은 본 개시에 따른 시스템 전체의 구성도이다.

도 2는 본 개시에 따른 컴플라이언스 수집 및 등록부를 도시한 도면이다.

도 3은 본 개시에 따른 컴플라이언스 수집 자동화 모듈을 도시한 도면이다.

도 4는 본 개시에 따른 컴플라이언스 인스펙트 모듈을 도시한 도면이다.

도 5는 본 개시에 따른 사내 컴플라이언스 인스펙트 자동화 모듈을 도시한 도면이다.

도 6은 본 개시에 따른 회사별 보안 요구사항 분석 자동화 모듈을 도시한 도면이다.

도 7은 본 개시에 따른 개인정보 수집 및 이용과 분석부를 도시한 도면이다.

도 8은 본 개시에 따른 수집폼 생성 및 응답 자동화 모듈을 도시한 도면이다.

도 9는 본 개시에 따른 개인정보 수집양식 생성 모듈을 도시한 도면이다.

도 10은 본 개시에 따른 개인정보 수집 감지 자동화 모듈을 도시한 도면이다.

도 11은 본 개시에 따른 수집 및 이용 동의서 자동 생성 모듈을 도시한 도면이다.

도 12는 본 개시에 따른 개인정보처리방침 자동 생성 모듈을 도시한 도면이다.

도 13은 본 개시에 따른 개인정보주체자 토큰 및 동의이력 해시 생성 모듈을 도시한 도면이다.

도 14는 본 개시에 따른 컴플라이언스 및 보안 위험도 분석부를 도시한 도면이다.

도 15는 본 개시에 따른 서비스별 개인정보 분석부를 도시한 도면이다.

도 16은 본 개시에 따른 개인정보 파기부를 도시한 도면이다.

도 17은 본 개시에 따른 인증 관리부를 도시한 도면이다.

도 18은 본 개시에 따른 수탁 업체 현황을 도시한 도면이다.

도 19는 본 개시에 따른 개인정보 처리 현황을 도시한 도면이다.

도 20은 본 개시에 따른 재위탁 업체 현황을 도시한 도면이다.

도 21은 본 개시에 따른 점검 체크리스트의 점검 항목을 설명한 도면이다.

도 22는 본 개시에 따른 점검 체크리스트의 점검 현황을 설명한 도면이다.

도 23은 본 개시에 따른 점검 체크리스트의 벌칙 규정을 설명한 도면이다.

도 24는 본 개시에 따른 컴플라이언스 요구 사항 분석 및 점검 자동화 장치의 구성도를 도시한 도면이다.

도 25는 본 개시에 따른 컴플라이언스 요구 사항 분석 및 점검 자동화 방법의 순서도를 도시한 도면이다.

도 26은 본 개시에 따른 본 발명의 핵심 개념을 도시한 도면이다.

도 27은 본 개시에 따른 조항별 주요 키워드를 도출하는 실시 예를 도시한 도면이다.

도 28은 본 개시에 따른 보안 요구사항의 컴플라이언스 준수 여부를 확인하는 실시 예를 도시한 도면이다.

도 29는 본 개시에 따른 위험도를 계산하고 위험 조치를 실행하는 실시 예를 도시한 도면이다.

도 30은 본 개시에 따른 종래기술의 문제점을 설명하는 실시 예를 도시한 도면이다.

도 31은 본 개시에 따른 처리방침 간단 검토 기능을 설명하는 실시 예를 도시한 도면이다.

도 32는 본 개시에 따른 처리방침 간단 검토 방법의 순서도를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 개시 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다. 본 개시가 실시예들의 모든 요소들을 설명하는 것은 아니며, 본 개시가 속하는 기술분야에서 일반적인 내용 또는 실시예들 간에 중복되는 내용은 생략한다. 명세서에서 사용되는 '부, 모듈, 부재, 블록'이라는 용어는 소프트웨어 또는 하드웨어로 구현될 수 있으며, 실시예들에 따라 복수의 '부, 모듈, 부재, 블록'이 하나의 구성요소로 구현되거나, 하나의 '부, 모듈, 부재, 블록'이 복수의 구성요소들을 포함하는 것도 가능하다.

[0030] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 직접적으로 연결되어 있는 경우뿐 아니라, 간접적으로 연결되어 있는 경우를 포함하고, 간접적인 연결은 무선 통신망을 통해 연결되는 것을 포함한다.

[0031] 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0032] 명세서 전체에서, 어떤 부재가 다른 부재 "상에" 위치하고 있다고 할 때, 이는 어떤 부재가 다른 부재에 접해 있는 경우뿐 아니라 두 부재 사이에 또 다른 부재가 존재하는 경우도 포함한다.

[0033] 제 1, 제 2 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하기 위해 사용되는 것으로, 구성요소가 전술된 용어들에 의해 제한되는 것은 아니다.

[0034] 단수의 표현은 문맥상 명백하게 예외가 있지 않는 한, 복수의 표현을 포함한다.

[0035] 각 단계들에 있어 식별부호는 설명의 편의를 위하여 사용되는 것으로 식별부호는 각 단계들의 순서를 설명하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않는 이상 명기된 순서와 다르게 실시될 수 있다.

[0036] 이하 첨부된 도면들을 참고하여 본 개시의 작용 원리 및 실시예들에 대해 설명한다.

[0037] 본 명세서에서 본 발명은 서버 시스템뿐만 아니라 연산처리를 수행하여 사용자에게 결과를 제공할 수 있는 다양한 장치들로 구현될 수 있다. 예를 들어, 본 발명은 컴퓨터, 서버 장치 및 휴대용 단말기를 모두 포함하거나, 또는 어느 하나의 형태가 될 수 있다.

[0038] 여기에서, 상기 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop), 태블릿 PC, 슬레이트 PC 등을 포함할 수 있다.

[0039] 상기 서버 장치는 외부 장치와 통신을 수행하여 정보를 처리하는 서버로써, 애플리케이션 서버, 컴퓨팅 서버, 데이터베이스 서버, 파일 서버, 게임 서버, 메일 서버, 프록시 서버 및 웹 서버 등을 포함할 수 있다.

[0040] 상기 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), WiBro(Wireless Broadband Internet) 단말, 스마트 폰(Smart Phone) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치와 시계, 반지, 팔찌, 발찌, 목걸이, 안경, 콘택트 렌즈, 또는 머리 착용형 장치(head-mounted-device(HMD) 등과 같은 웨어러블 장치를 포함할 수 있다.

[0041] 본 개시에 따른 인공 지능과 관련된 기능은 프로세서와 메모리를 통해 동작된다. 프로세서는 하나 또는 복수의 프로세서로 구성될 수 있다. 이때, 하나 또는 복수의 프로세서는 CPU, AP, DSP(Digital Signal Processor) 등과 같은 범용 프로세서, GPU, VPU(Vision Processing Unit)와 같은 그래픽 전용 프로세서 또는 NPU와 같은 인공 지능 전용 프로세서일 수 있다. 하나 또는 복수의 프로세서는, 메모리에 저장된 기 정의된 동작 규칙 또는 인공 지능 모델에 따라, 입력 데이터를 처리하도록 제어한다. 또는, 하나 또는 복수의 프로세서가 인공 지능 전용 프로세서인 경우, 인공 지능 전용 프로세서는, 특정 인공 지능 모델의 처리에 특화된 하드웨어 구조로 설계될 수 있다.

[0042] 기 정의된 동작 규칙 또는 인공 지능 모델은 학습을 통해 만들어진 것을 특징으로 한다. 여기서, 학습을 통해 만들어진다는 것은, 기본 인공 지능 모델이 학습 알고리즘에 의하여 다수의 학습 데이터들을 이용하여 학습됨으로써, 원하는 특성(또는, 목적)을 수행하도록 설정된 기 정의된 동작 규칙 또는 인공 지능 모델이 만들어짐을 의미한다. 이러한 학습은 본 개시에 따른 인공 지능이 수행되는 기기 자체에서 이루어질 수도 있고, 별도의 서버 및/또는 시스템을 통해 이루어 질 수도 있다. 학습 알고리즘의 예로는, 지도형 학습(supervised learning),

비지도 형 학습(unsupervised learning), 준지도형 학습(semi-supervised learning) 또는 강화 학습(reinforcement learning)이 있으나, 전술한 예에 한정되지 않는다.

[0043] 인공 지능 모델은, 복수의 신경망 모듈들로 구성될 수 있다. 복수의 신경망 모듈들 각각은 복수의 가중치들(weight values)을 갖고 있으며, 이전(previous) 모듈의 연산 결과와 복수의 가중치들 간의 연산을 통해 신경망 연산을 수행한다. 복수의 신경망 모듈들이 갖고 있는 복수의 가중치들은 인공 지능 모델의 학습 결과에 의해 최적화될 수 있다. 예를 들어, 학습 과정 동안 인공 지능 모델에서 획득한 로스(loss) 값 또는 코스트(cost) 값이 감소 또는 최소화되도록 복수의 가중치들이 갱신될 수 있다. 인공 신경망은 심층 신경망(DNN:Deep Neural Network)를 포함할 수 있으며, 예를 들어, CNN (Convolutional Neural Network), DNN (Deep Neural Network), RNN (Recurrent Neural Network), RBM (Restricted Boltzmann Machine), DBN (Deep Belief Network), BRDNN(Bidirectional Recurrent Deep Neural Network) 또는 심층 Q-네트워크 (Deep Q-Networks) 등이 있으나, 전술한 예에 한정되지 않는다.

[0044] 프로세서는 뉴럴 네트워크를 생성하거나, 뉴럴 네트워크를 훈련(train, 또는 학습(learn)하거나, 수신되는 입력 데이터를 기초로 연산을 수행하고, 수행 결과를 기초로 정보 신호(information signal)를 생성하거나, 뉴럴 네트워크를 재훈련(retrain)할 수 있다.

[0045] 뉴럴 네트워크는 CNN(Convolutional Neural Network), RNN(Recurrent Neural Network), 퍼셉트론(perceptron), 다층 퍼셉트론(multilayer perceptron), FF(Feed Forward), RBF(Radial Basis Network), DFF(Deep Feed Forward), LSTM(Long Short Term Memory), GRU(Gated Recurrent Unit), AE(Auto Encoder), VAE(Variational Auto Encoder), DAE(Denoising Auto Encoder), SAE(Sparse Auto Encoder), MC(Markov Chain), HN(Hopfield Network), BM(Boltzmann Machine), RBM(Restricted Boltzmann Machine), DBN(Depp Belief Network), DCN(Deep Convolutional Network), DN(Deconvolutional Network), DCIGN(Deep Convolutional Inverse Graphics Network), GAN(Generative Adversarial Network), LSM(Liquid State Machine), ELM(Extreme Learning Machine), ESN(Echo State Network), DRN(Deep Residual Network), DNC(Differentiable Neural Computer), NTM(Neural Turning Machine), CN(Capsule Network), KN(Kohonen Network) 및 AN(Attention Network)를 포함할 수 있으나 이에 한정되는 것이 아닌 임의의 뉴럴 네트워크를 포함할 수 있음은 통상의 기술자가 이해할 것이다.

[0046] 본 개시의 예시적인 실시예에 따르면, 프로세서는 GoogleNet, AlexNet, VGG Network 등과 같은 CNN(Convolution Neural Network), R-CNN(Region with Convolution Neural Network), RPN(Region Proposal Network), RNN(Recurrent Neural Network), S-DNN(Stacking-based deep Neural Network), S-SDNN(State-Space Dynamic Neural Network), Deconvolution Network, DBN(Deep Belief Network), RBM(Restrcted Boltzman Machine), Fully Convolutional Network, LSTM(Long Short-Term Memory) Network, Classification Network, Generative Modeling, eXplainable AI, Continual AI, Representation Learning, AI for Material Design, 자연어 처리를 위한 BERT, SP-BERT, MRC/QA, Text Analysis, Dialog System, GPT-3, GPT-4, 비전 처리를 위한 Visual Analytics, Visual Understanding, Video Synthesis, ResNet 데이터 지능을 위한 Anomaly Detection, Prediction, Time-Series Forecasting, Optimization, Recommendation, Data Creation 등 다양한 인공 지능 구조 및 알고리즘을 이용할 수 있으며, 이에 제한되지 않는다. 이하, 첨부된 도면을 참조하여 본 개시의 실시예를 상세하게 설명한다.

[0047] 도 1은 본 개시에 따른 시스템 전체의 구성도이다.

[0048] 도 1(10)을 참조하여, 시스템 전체의 구성을 설명한다.

[0049] 시스템(10)은 간략하게 A부(100), B부(200), C부(300), D부(400), E부(500), F부(600) 및 프로세서(50)로 구성된다.

[0050] A부(100)는 컴플라이언스 수집 및 등록부로 명칭될 수 있다.

[0051] B부(200)는 개인정보 수집 및 이용과 분석부로 명칭될 수 있다.

[0052] C부(300)는 컴플라이언스 및 보안 위험도 분석부로 명칭될 수 있다.

[0053] D부(400)는 서비스별 개인정보 분석부로 명칭될 수 있다.

[0054] E부(500)는 개인정보 파기부로 명칭될 수 있다.

[0055] F부(600)는 인증관리부로 명칭될 수 있다.

[0056] 프로세서(50)는 A부(100), B부(200), C부(300), D부(400), E부(500) 및 F부(600)를 제어한다.

[0057] A부(100), B부(200), C부(300), D부(400), E부(500) 및 F부(600) 중 적어도 하나의 세부 기능은 소프트웨어로 메모리에 저장될 수 있고, 프로세서(50)는 메모리를 참조하여 개별 부의 세부 기능을 실행할 수 있다.

[0058] 본 발명의 핵심 용어를 정의한다.

[0059] 컴플라이언스는 통상 법규준수, 준법감시, 내부통제 등의 의미로 컴플라이언스 프로그램이란 사업 추진 과정에서 기업이 자발적으로 관련 법규를 준수하도록 하기 위한 일련의 시스템이다. 컴플라이언스는 보안규제를 포함한다.

[0060] 규제는 법, 시행령, 고시, 가이드 등을 포함한다.

[0061] 인스펙트는 구축을 의미하고, 조사는 조사를 위해서 통제항목을 생성 및 구성하는 행위, 즉, 기준 수립을 위한 행위를 의미한다.

[0062] 통제항목은 개인정보 보호를 위해서 기관이 반드시 준수하여야 할 항목을 의미한다.

[0063] 트리거는 발생조건을 의미한다.

[0064] 태그는 주요 키워드를 의미한다.

[0065] 사내 컴플라이언스는 내규를 의미한다.

[0066] 보안요구사항은 정보 자산을 보호하기 위해 기관(기업) 또는 서비스의 상황별로 요청되는 보안기준 및 보안규칙을 의미한다.

[0067] 공통규제는 국가별 규제들 중에 존재하는 공통점으로 국가별 공통규제, 업종별 공통규제를 포함한다.

[0068] 국가별 공통규제는 기관, 기업이 선택한 국가별로 존재하는 규제들 중 공통적으로 존재하는 규제를 의미한다.

[0069] 업종별 공통규제는 기관, 기업이 선택한 업종, 산업, 규모에 요구되는 규제들 중 공통적으로 존재하는 규제를 의미한다.

[0070] 마이크로 규제는 다수의 규제들 중에 차이점이 있는 규제이다.

[0071] 예를 들어, 마이크로 규제는 기관, 기업이 선택한 규제들 중 기관이 개별적으로 준수해야 하는 규제이거나, 또는 법령에 구체적 정함이 없는 규제, 구체적인 시기, 방법이 정해지지 않은 사항들이 될 수 있다.

[0072] 도 2는 본 개시에 따른 컴플라이언스 수집 및 등록부를 도시한 도면이다.

[0073] 도 2(210)를 참조하여, 컴플라이언스 수집 및 등록부(100)를 설명한다.

[0074] 컴플라이언스 수집 및 등록부(100)는 약칭으로 A부(100)가 된다.

[0075] A1 모듈(110)은 컴플라이언스 수집 자동화 모듈로 명칭될 수 있고, A2 모듈(120)은 컴플라이언스 인스펙트 자동화 모듈로 명칭될 수 있고, A3 모듈은 회사별 보안 요구사항 분석 자동화 모듈로 명칭될 수 있다.

[0076] 도 3은 본 개시에 따른 컴플라이언스 수집 자동화 모듈을 도시한 도면이다.

[0077] 도 3(310)을 참조하여, 컴플라이언스 수집 자동화 모듈(110)을 설명한다.

[0078] 컴플라이언스 수집 자동화 모듈(110)는 국가별로 개인정보와 관련된 규제를 찾아내고, 규제 조항을 분류하고, 해당 조항들에 등장하는 '주어', '목적어', '서술어'를 본문과 단서조항으로 나누어 분석한다.

[0079] 컴플라이언스 수집 자동화 모듈(110)은 분석에 따라서 키워드를 설정하고 이를 태그로 만든다.

[0080] 컴플라이언스 수집 자동화 모듈(110)은 컴플라이언스 수집 모듈(111), 컴플라이언스 분석-정제 ML 모듈(112)를 포함한다.

[0081] 컴플라이언스 수집 모듈(111)은 Crawler, Scraper, API를 포함한다.

[0082] 컴플라이언스 분석-정제 ML모듈(112)은 분석에 따라서 키워드를 설정하고 이를 태그로 만든다. Vision AI, NLP AI, ETC를 포함한다.

[0083] 컴플라이언스 분석-정제 ML모듈(112)은 다음을 수행한다.

[0084] 첫째, 우선 순위를 결정한다.

[0085] 1) 본문인지 단서조항인지, 2) 일반법인지, 특별법인지에 따른 규제간 우선순위, 3) 법령체계에 따른 규제간 적용의 우선순위를 결정한다.

[0086] 둘째, 주어, 목적어, 동사 판단 및 태깅을 수행한다.

[0087] 1) 조항별 '법 주어' 정의하기는 법조문의 주어에 해당하는 것을 법조문의 인용관계를 기반으로 판단하는 것을 의미한다.

[0088] 2) 조항별 '법 목적어' 정의하기는 법조문의 목적어에 해당하는 것을 법조문의 인용관계를 기반으로 판단하는 것을 의미한다.

[0089] 3) '동사'를 정의한다.

[0090] 셋째, 법제차이 판단 및 태깅을 수행한다.

[0091] 1) 특정한 규제 (법률, 시행령, 시행규칙, 고시, 훈령, 예규 등) 에 관해서 국가간 차이점을 판단한다.

[0092] 여기서, 규제는 다음 내용을 포함한다.

[0093] 법률 (Act, Law, Statute)은 국회의 입법 과정을 통해 제정된 법으로, 영어로는 "Act" 또는 "Law", "Statute"로 번역된다. 예를 들어, "민법"은 "Civil Act"로 번역될 수 있다.

[0094] 시행령 (Enforcement Decree)은 법률을 구체적으로 시행하기 위한 대통령령을 의미하며, 영어로는 "Enforcement Decree"라고 번역된다.

[0095] 시행규칙 (Enforcement Rule)은 시행령을 보다 세부적으로 규정하는 부처의 규칙을 의미하며, 영어로는 "Enforcement Rule"로 번역된다.

[0096] 고시 (Public Notice, Notification)는 특정 사항을 알리기 위해 발행되며 "Public Notice" 또는 "Notification"으로 번역된다.

[0097] 훈령 (Directive, Instruction)은 상급 기관에서 하급 기관에 대한 지시를 내리는 행정명령으로, "Directive" 또는 "Instruction"으로 번역된다.

[0098] 예규 (Regulation, Official Instruction)는 행정 기관 내의 절차나 업무에 관한 규정을 담은 것으로 "Regulation" 또는 "Official Instruction"으로 번역될 수 있다.

[0099] 국가별 개인정보 법령 (법, 시행령, 규칙, 고시, 훈령, 예규)관리모듈(미도시)은 국가별 개인정보 관련규제를 빠르게 판단할 수 있도록 가공한다

[0100] 도 4는 본 개시에 따른 컴플라이언스 인스펙트 모듈을 도시한 도면이다.

[0101] 도 4(410)를 참조하여, 컴플라이언스 인스펙트 모듈(120)에 대하여 설명한다.

[0102] 컴플라이언스 인스펙트 모듈(120)은 기관이 준수해야 하는 개인정보보호와 관련된 통제항목을 맞춤형으로 구축하고 생성한다.

[0103] 컴플라이언스 인스펙트 모듈(120)은 A1 모듈(110)에서 1) 수집, 정제된 '국가별 컴플라이언스' 와 2) 보안요구사항을 고려하여 통제항목을 생성한다.

[0104] 컴플라이언스 인스펙트 모듈(120)은 국가별 컴플라이언스 인스펙트 트리거 자동화 모듈(121)과 내규 생성모듈(122)를 포함한다.

[0105] 국가별 컴플라이언스 인스펙트 트리거 자동화 모듈(121)은 국가별로 개인정보보호 규제(컴플라이언스)를 조사해서 (방법은 조항 하나하나에 적당한 tag를 붙이는것 임) 조사한 규제 태그가 마이크로 규제일지 공통규제인지를 나눈다.

[0106] 내규 생성모듈(122)은 사내 컴플라이언스에 맞게 마이크로규제를 선택하고, 선택된 마이크로규제를 기반으로 내규를 생성한다.

[0107] 내규 생성모듈(122)는 사내 보안담당자가 1차 모듈에서 나온 값을 보고, 내규에 맞는 마이크로 규제를

선택하고, 선택된 규제로 사내 내규를 생성한다.

[0108] 도 5는 본 개시에 따른 사내 컴플라이언스 인스펙트 자동화 모듈을 도시한 도면이다.

[0109] 도 5(510)를 참조하여, 사내 컴플라이언스 인스펙트 자동화 모듈(123)을 설명한다.

[0110] 사내 컴플라이언스 인스펙트 자동화 모듈(123)은 내규를 인스펙트 자동화 모듈(점검항목으로)로 만들어서 점검을 유무를 On, Off 할 수 있도록 한다.

[0111] 사내 컴플라이언스 인스펙트 자동화 모듈(123)은 B2 모듈(220)과 연결될 수 있다.

[0112] 도 6은 본 개시에 따른 회사별 보안 요구사항 분석 자동화 모듈을 도시한 도면이다.

[0113] 도 6(610)를 참조하여, 회사별 보안 요구사항 분석 자동화 모듈(130)을 설명한다.

[0114] 회사별 보안 요구사항 분석 자동화 모듈(130)은 비즈니스 보안 요구사항 분석 모듈(131)을 포함한다. 여기서 회사는 기관도 포함한다.

[0115] 회사별 보안 요구사항 분석 자동화 모듈(130)은 기관정보를 획득하고, 서비스 정보를 획득한다.

[0116] 위치에서 국가 정보를 획득하고, 회사명, 규모, 회사식별번호, 서비스 정보를 획득한다.

[0117] 비즈니스 보안요구사항 분석모듈(131)은 획득 정보를 기초로 어떤 규제에 해당할지 판단한다.

[0118] 구체적으로, 비즈니스 보안요구사항 분석모듈(131)은 (획득된) 기관/서비스 정보를 기준으로 어떠한 규제가 적용될지 판단한다.

[0119] 도 7은 본 개시에 따른 개인정보 수집 및 이용과 분석부를 도시한 도면이다.

[0120] 도 7(710)을 참조하여, 개인정보 수집 및 이용과 분석부(200)에 대하여 설명한다.

[0121] 개인정보 수집 및 이용과 분석부(200)는 B부(200)에 대응된다.

[0122] B부(200)는 B1 모듈(210), B2 모듈(220), B3 모듈(230), B4 모듈(240) 및 B5 모듈(250)을 포함한다.

[0123] B1 모듈(210)은 수집폼 생성 및 응답 자동화 모듈로 명칭될 수 있고, B2 모듈(220)은 개인정보 수집 감지 자동화 모듈로 명칭될 수 있고, B3 모듈(230)은 수집 및 이용 동의서 자동 생성 모듈로 명칭될 수 있고, B4 모듈(240)은 개인정보처리방침 자동 생성 모듈로 명칭될 수 있고, B5 모듈(250)은 개인정보주체자 토큰 및 동의이력 해시 생성 모듈로 명칭될 수 있다.

[0124] 도 8은 본 개시에 따른 수집폼 생성 및 응답 자동화 모듈을 도시한 도면이다.

[0125] 도 8(810)을 참조하여, 수집폼 생성 및 응답 자동화 모듈(210)을 설명한다.

[0126] 수집폼 생성 및 응답 자동화 모듈(210)은 관리자가 입력 양식을 생성하고, 정보주체로부터 개인정보를 수집한다.

[0127] 수집폼 생성 및 응답 자동화 모듈(210)은 개인정보 수집양식 생성 모듈(211), 개인정보 수집여부 감지모듈(212), 사내 컴플라이언스 구축모듈(213), 처리 근거 생성모듈(214) 및 개인정보 처리방침 생성모듈(215)를 포함한다.

[0128] 개인정보 수집양식 생성 모듈(211)은 콘텐츠(text, image, video)를 수집하고, 응답방법(전자서명, 본인인증 유무)을 결정하고, 정보수집목록 및 유형을 생성한다.

[0129] 개인정보 수집여부 감지모듈(212)는 개인정보를 수집하는 양식에서 수집되는개인정보가 실제 개인정보인지 여부를 판단하고, 수집된 정보가 개인정보에 해당하는 경우, 개인정보 수집 감지를 담당하는 '수집행위 관리부'에 해당 정보를 전달한다.

[0130] 사내 컴플라이언스 구축모듈(213)은 사내 컴플라이언스를 조사한다.

[0131] 사내 컴플라이언스 구축모듈(213)은 기업정보와 서비스정보를 기반으로 기관의 내규에 저촉되는지를 판단하는 역할을 한다. 조사를 하기 때문에, 인스펙트를 수행한다고 할 수 있다.

[0132] 처리 근거 생성모듈(214)은 개인정보 수집 및 이용 동의서를 자동으로 생성한다.

[0133] 처리 근거 생성모듈(214)은 개인정보 수집/제공 동의서 및 이용 동의서 또는 처리의 근거를 자동 생성 한다. 기

관정보와 서비스정보를 기반으로 개인정보 수집/제공 동의서 및 개인정보 이용 동의서를 생성하기 때문에 맞춤형으로 동의서를 생성할 수 있다. 개인정보를 제공하는 정보주체의 정보를 기반으로 동의서를 맞추는 등 수정이 가능하다.

[0134] 처리 근거는 다음과 같다.

[0135] 1. 정보주체의 동의를 받은 경우이다.

[0136] 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우이다.

[0137] 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우이다.

[0138] 4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우이다.

[0139] 5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우이다.

[0140] 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

[0141] 7. 공중위생 등 공공의 안전과 안녕을 위한 경우이다.

[0142] 개인정보 처리방침 생성모듈(215)은 개인정보 처리방침을 자동으로 생성한다.

[0143] 개인정보 처리방침 생성모듈(215)은 기관정보와 서비스정보를 기반으로 개인정보 처리방침을 자동으로 생성하며, 개인정보를 제공하는 정보주체의 정보를 기반으로 개인정보 처리방침을 맞춤형으로 생성할 수 있다. 생성된 개인정보 처리방침은 '처리방침 관리부'로 전달되어 관리가 이루어진다.

[0144] 도 9는 본 개시에 따른 개인정보 수집양식 생성 모듈을 도시한 도면이다.

[0145] 도 9는 도 9(a), 도 9(b) 및 도 9(c)를 포함한다.

[0146] 도 9(a)(910)은 개인정보 수집양식 생성 모듈(211)을 도시한 도면이다.

[0147] 도 9(b)(920)은 개인정보 수집여부 감지모듈(212), 사내 컴플라이언스 구축모듈(213), 처리 근거 생성모듈(214)를 도시한 도면이다.

[0148] 도 9(c)(930)은 개인정보 처리방침 생성모듈(215)를 도시한 도면이다.

[0149] 도 9(a)(910)에 도시한 바와 같이, 개인정보 수집양식 생성모듈(211)은 개인정보를 수입하기 위한 양식을 생성하는데, 사내 서비스 관리자가 기관정보와 서비스정보를 기반으로 선택할 수 있으며, 자동으로 개인 정보 수집 양식을 생성한다(S1).

[0150] 도 9(b)(920)에 도시한 바와 같이, 개인정보 수집여부 감지모듈(212)은 개인정보를 수집하는 양식에서 수집되는 정보가 개인정보인지 개인정보가 아닌지를 판단하고, 수집된 정보가 개인정보에 해당할 경우, 개인정보 수집 감지를 담당하는 '수집행위 관리부'에 해당 정보를 전달하는 역할을 한다(S2).

[0151] 사내 컴플라이언스 구축모듈(213)은 기업정보와 서비스정보를 기반으로 기관의 내규에 저촉되는지를 판단하는 역할을 한다. 조사를 하기 때문에, 인스펙트를 수행한다(S3).

[0152] 처리 근거 생성모듈(214)은 개인정보 수집/제공 동의서 또는 처리의 근거를 자동 생성하는 역할을 한다(S4). 기관정보와 서비스정보를 기반으로 개인정보 수집/제공 동의서를 생성하기 때문에 맞춤형으로 동의서를 생성할 수 있다. 개인정보를 제공하는 정보주체의 정보를 기반으로 동의서를 맞추는 등 수정이 가능하다.

[0153] 처리 근거는 다음과 같다.

[0154] 1. 정보주체의 동의를 받은 경우이다.

[0155] 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우이다.

[0156] 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우이다.

[0157] 4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기

위하여 필요한 경우이다.

[0158] 5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우이다.

[0159] 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

[0160] 7. 공중위생 등 공공의 안전과 안녕을 위함이다.

[0161] 도 9(c)(930)에 도시한 바와 같이, 개인정보 처리방침 생성모듈(215)은 기관정보와 서비스정보를 기반으로 개인정보 처리방침을 자동으로 생성하고, 이를 '처리방침 관리부'로 전달하여 관리한다(S5).

[0162] 도 10은 본 개시에 따른 개인정보 수집 감지 자동화 모듈을 도시한 도면이다.

[0163] 도 10(1010)을 참조하면, 개인정보 수집 감지 자동화 모듈(220)은 개인정보 수집 요청 여부 감지 AI 인스펙트 모듈(221), 개인정보 제출 여부 감지 AI 인스펙트 모듈(222)를 포함한다.

[0164] 개인정보 수집 감지 자동화 모듈(220)은 B1 모듈(210)의 개인정보 수집여부 감지모듈(212)과 연동된다.

[0165] 개인정보 수집 감지 자동화 모듈(220)은 사내 컴플라이언스 인스펙트 자동화 모듈(123)과 연동된다.

[0166] 개인정보 수집 감지 자동화 모듈(220)은 개인정보 수집 요청이 발생했는지 여부를 감지하고, 수집된 정보가 실제 개인정보에 해당하는지 판단하여 이를 관리한다. 개인정보는 민감정보, 고유식별번호, 주민번호 등을 포함한다.

[0167] 개인정보 수집 요청 여부 감지 AI 인스펙트 모듈(221)은 개인정보의 유형에 따라 (예: 개인정보, 민감정보, 고유식별번호 등) 수집되는 정보의 종류를 자동으로 분류하고, 각 유형에 따른 적합한 처리 절차를 자동으로 적용한다.

[0168] 개인정보 제출 여부 감지 AI 인스펙트 모듈(222)은 원치않는, 불필요한, 의도하지 않는 개인정보 수집을 방지하기 위하여 사용자가 제공한 정보가 개인정보에 해당하는지 AI 기반 분석(예: Vision AI, NLP AI 등)을 통해 판단하고, 수집 여부를 감지한다.

[0169] 개인정보 제출 여부 감지 AI 인스펙트 모듈(222)은 사용자의 입력 데이터를 Vision AI, NLP AI 등 다양한 인공지능 기술을 활용하여 분석하고, 입력된 정보가 개인정보에 해당하는지 실시간으로 판단한다.

[0170] 도 11은 본 개시에 따른 수집 및 이용 동의서 자동 생성 모듈을 도시한 도면이다.

[0171] 도 11(1110)을 참조하여, 수집 및 이용 동의서 자동 생성 모듈(230)에 대하여 설명한다.

[0172] 수집 및 이용 동의서 자동 생성 모듈(230)은 B3 모듈(230)에 대응한다.

[0173] 수집 및 이용 동의서 자동 생성 모듈(230)은 처리 안내서, 수집 및 이용 동의서 생성 자동화 모듈(231), 동의서 유형 템플릿 반영 자동화 모듈(232) 및 개인정보 수집 목적 분석 모듈(233)을 포함한다.

[0174] 수집 및 이용 동의서 자동 생성 모듈(230)은 개인정보의 수집과 처리 과정에서 필요한 동의서를 자동으로 생성하고 관리하는 시스템이다. 개인정보의 유형 및 수집 목적을 분석하여 적합한 동의서 템플릿을 자동으로 적용하며, 법적 요구 사항을 반영한 맞춤형 동의서를 생성하여 정보주체로부터 동의를 받는 과정을 자동화함으로써 개인정보 보호 규정을 준수한다.

[0175] 본 발명의 동작 흐름에 대하여 설명한다.

[0176] 첫째, B2 모듈(220)이 분류한 개인정보의 종류에 따라 개인정보 동의서의 종류를 선정한다.

[0177] 둘째, 동의서 내 포함되어야할 정보를 개인정보처리자에게 직접 입력받는다.

[0178] 1. 개인정보의 처리목적이 동의서를 생성하지 않는 조건에 해당할 경우 동의근거를 생성한다.

[0179] 2. 동의서를 생성하는 조건에서는 동의서 내 개인정보의 처리목적은 개인정보 수집양식 생성모듈의 값을 참고하여 개인정보 수집목적 분석 모듈에서 목적을 제안한다.

[0180] 3. 상기 내용과 개인정보처리자가 선택한 템플릿으로 동의서를 생성한다.

[0181] 처리 안내서, 수집 및 이용 동의서 생성 자동화 모듈(231)은 개인정보와 민감정보, 고유식별정보 등과 관련된

동의서와 처리 안내서를 자동으로 생성하는 역할을 수행한다. 동의서와 안내서는 다음과 같은 형식으로 구분된다.

[0182] 1) 개인정보 수집 및 이용 동의서의 경우, 일반 개인정보(이름, 전화번호, 이메일 등)를 수집하는 경우 생성되며, 수집 항목, 목적, 보관 기간, 동의거부권 및 그 불이익 등이 포함된다.

[0183] 2) 민감정보 수집 및 이용 동의서의 경우, 건강 정보, 금융 정보 등 민감한 개인정보를 수집할 때 사용되며, 관련 법률에 따른 고지사항 및 추가 동의 의사 요청이 포함된다.

[0184] 3) 고유식별정보 수집 및 이용 동의서의 경우, 외국인등록번호, 여권번호, 운전면허번호와 같은 고유식별번호를 수집하는 경우 생성되며, 관련 법률에 따른 고지사항 및 추가 동의 항목의사 요청이 포함된다.

[0185] 4) 주민등록번호 처리 안내서의 경우, 주민등록번호와 같은 고유한 식별번호를 처리할 때 제공되는 안내서로, 처리 목적과 법적 근거가 명확히 고지된다.

[0186] 5) 선택 동의서의 경우, 광고 등 필수 목적으로 수집하는 개인정보가 아닌 선택적으로 개인정보를 수집하는 경우 생성되며 수집 항목, 목적, 보관 기간, 동의거부권 및 그 불이익 등이 포함된다.

[0187] 처리 안내서, 수집 및 이용 동의서 생성 자동화 모듈(231)은 정보주체가 동의서를 이해하고 동의 여부를 쉽게 선택할 수 있도록 직관적인 인터페이스를 제공하며, 동의서의 각 항목은 관련 법률과 규제에 맞춰 업데이트된다.

[0188] 동의서 유형 템플릿 반영 자동화 모듈(232)은 다양한 유형의 동의서와 처리 안내서 템플릿을 사전에 정의하고, 사용자가 선택한 개인정보 수집 목적 및 법적 요구 사항에 따라 적합한 템플릿을 자동으로 반영한다. 해당 모듈의 주요 기능은 다음과 같다.

[0189] 첫째, 동의서 템플릿 관리이다.

[0190] 개인정보의 수집 유형에 따라 각기 다른 템플릿을 제공하며, 서비스 목적에 따라 맞춤형 동의서를 생성한다. 예를 들어, 온라인 서비스 가입 시 필요한 개인정보와 오프라인 거래에서 필요한 개인정보에 따라 다른 템플릿을 적용할 수 있다.

[0191] 둘째, 템플릿 반영 규칙이다.

[0192] 특정 정보 유형이 입력될 때 이에 맞는 템플릿을 자동으로 선택하는 규칙과 개인정보취급자의 선택을 기반으로 동작한다. 예를 들어, 건강정보 수집 시에는 민감정보 템플릿을 적용하고, 단순 연락처 수집 시에는 개인정보 템플릿을 적용하는 방식이다.

[0193] 셋째, 법적 규제 자동 반영이다.

[0194] 국가별, 산업별 법적 규제를 미리 정의된 규칙에 따라 동의서 템플릿에 반영한다. 예를 들어, GDPR(유럽 개인정보 보호법)을 적용하는 경우와 CCPA(캘리포니아 소비자 개인정보 보호법)을 적용하는 경우에 맞게 동의서 내용이 반영된다.

[0195] 동의서 유형 템플릿 반영 자동화 모듈(232)은 지속적으로 업데이트되며, 새로운 법률이나 규정이 발표될 경우 해당 내용을 템플릿에 즉각 반영할 수 있다.

[0196] 개인정보 수집 목적 분석 모듈(233)은 Vision AI, NLP AI, 및 기타 인공지능 기술을 활용하여, 사용자가 입력한 정보를 분석하고 그에 따른 개인정보 수집 목적을 자동으로 분류하고 처리한다. 주요 기능은 다음과 같다.

[0197] 첫째, Vision AI 기반 이미지 분석이다.

[0198] 개인정보 수집 양식에 이미지가 포함된 경우, 이미지 내 텍스트나 이미지 등에서 주제를 추출하고 분석하여 적합한 목적을 제안한다. 예를 들어, 행사포스터 이미지에서 행사 진행의 주제를 추출하면, 이에 맞는 목적을 추천한다.

[0199] 둘째, NLP AI 기반 텍스트 분석이다.

[0200] 사용자가 입력한 텍스트 데이터를 분석하여, 수집 목적을 파악한다. 예를 들어, 사용자가 온라인 가입 페이지를 생성하기위해 입력한 정보를 분석하여, 그 목적이 서비스 가입 목적임을 추천한다.

[0201] 셋째, 목적별 동의서 추천이다.

[0202] 수집된 정보를 바탕으로, 해당 정보가 어떤 법적 요구사항을 충족해야 하는지를 분석하고, 이에 맞는 목적을 추천한다. 예를 들어, 경품 당첨자의 개인정보 수집양식에 주민등록번호를 수집하면 세금신고 목적을 추천한다.

[0203] 개인정보 수집 목적 분석 모듈(233)은 수집된 개인정보의 처리 목적을 정확하게 분석하고, 개인정보 보호법에 따라 적합한 처리 방법을 적용하여 정보주체에게 알리고 동의를 받을 수 있도록 돕는다.

[0204] 도 12는 본 개시에 따른 개인정보처리방침 자동 생성 모듈을 도시한 도면이다.

[0205] 도 12(1210)를 참조하여, 개인정보처리방침 자동 생성 모듈(240)에 대하여 설명한다.

[0206] 개인정보처리방침 자동 생성 모듈(240)은 B4 모듈(240)에 대응된다.

[0207] 개인정보처리방침 자동 생성 모듈(240)은 서비스 분석 모듈(241), 처리방침 구성 요소 생성 모듈(242), 처리방침 탬플릿 반영 자동화 모듈(243)을 포함한다.

[0208] 개인정보처리방침 자동 생성 모듈(240)은 개인정보 처리방침을 자동으로 생성하고 관리하는 모듈로, 서비스 분석부터 처리방침 템플릿 반영까지 모든 절차를 자동화하는 역할을 수행한다. 이 모듈은 개인정보 처리와 관련된 법적 요구사항을 충족하며, 기업의 서비스 특성 및 보안 요건에 맞춘 처리방침을 자동으로 생성하는 것이 특징이다.

[0209] 개인정보처리방침 자동 생성 모듈(240)은 개인정보 처리방침을 자동으로 생성하고 관리하는 모듈이다. 서비스 분석 모듈을 통해 서비스의 특성을 파악하고, 처리방침 구성 요소를 자동으로 생성하며, 이를 템플릿에 반영하여 최종 처리방침을 완성한다. 이 시스템은 개인정보 처리 과정에서 발생하는 법적 요구 사항을 충족시키며, 서비스 제공자의 특성에 맞춘 맞춤형 처리방침을 제공함으로써 개인정보 보호와 관련된 법적 규제를 효과적으로 준수할 수 있다.

[0210] 개인정보처리방침 자동 생성 모듈(240)은 3개의 모듈로 구성되며 각각의 모듈은 처리방침의 구성과 자동화된 관리 절차를 효율적으로 수행한다.

[0211] 다른 모듈과 연계한 동작 흐름에 대하여 설명한다.

[0212] 첫째, 사용자에게 서비스의 현황을 제공받아 해당업종 등 그 현황과 관련된 처리방침의 요구사항을 분석한다.

[0213] 둘째, 사용자에게 개인정보처리현황을 제공받아 그 현황과 관련된 처리방침의 요구사항을 분석한다.

[0214] 셋째, 제공받은 정보를 바탕으로 개인정보처리방침을 구성한다.

[0215] 넷째, 이때 이용자가 선택한 템플릿을 적용하여 개인정보처리방침을 출력한다.

[0216] 서비스 분석 모듈(241)은 기업이나 서비스 제공자의 특성에 맞는 개인정보 처리방침을 구성하기 위해 서비스의 규모, 업종, 보안 요구사항 등을 분석하는 역할을 한다. 주요 기능은 다음과 같다.

[0217] 첫째, 업종 분석이다.

[0218] 서비스가 속한 업종을 분석하여, 해당 업종의 규제 및 법적 요구사항을 자동으로 반영한다. 예를 들어, 금융 서비스와 헬스케어 서비스는 서로 다른 법적 요건을 요구하기 때문에 각각의 업종에 맞는 처리방침을 자동으로 구분하고 생성한다.

[0219] 둘째, 서비스 규모 분석이다.

[0220] 기업의 규모에 따라 개인정보 처리방침의 복잡성과 요구사항이 달라진다. 이 모듈은 대기업, 중소기업, 스타트업 등 서비스 제공자의 규모를 분석하여 적절한 처리방침을 선택한다. 대규모 서비스의 경우 복잡한 데이터 처리 정책을 적용하고, 소규모 서비스는 단순화된 처리방침을 적용할 수 있다.

[0221] 셋째, 기타 변수 분석(ETC)이다.

[0222] 서비스 제공자의 비즈니스 모델, 고객 범위, 국제적 데이터 전송 여부 등을 포함한 다양한 요소를 분석한다. 예를 들어, 글로벌 서비스를 제공하는 경우 국경 간 데이터 이전에 대한 법적 요구사항이 처리방침에 반영된다.

[0223] 처리방침 구성 요소 생성 모듈(242)은 서비스 분석 모듈에서 제공된 데이터를 기반으로, 처리방침의 주요 구성 요소를 자동으로 생성한다. 이 모듈은 처리방침의 각 항목을 세부적으로 설계하며, 기업의 운영 방침에 맞게 이를 조정할 수 있다. 주요 기능은 다음과 같다.

[0224] 첫째, 개인정보 수집 및 이용과 제공이다.

[0225] 개인정보를 수집하는 목적, 수집되는 정보의 종류, 정보주체로부터의 동의나 동의받지 않은 사항을 정의한다. 이 항목은 기업이 수집하는 개인정보의 사용 범위와 타사에 제공되는 방식 등을 포함하며, 정보주체에게 명확히 고지되도록 설계된다.

[0226] 둘째, 가명정보 처리 여부이다.

[0227] 가명정보를 사용하는 기업의 경우, 가명 처리된 개인정보의 사용 범위와 처리 방법을 자동으로 정의한다. 이 항목은 가명 처리가 필요한 데이터의 종류와 사용 목적에 따라 맞춤형으로 설계되며, 필요 시 법적 근거도 함께 제공된다.

[0228] 셋째, 정보 보유 및 파기 정책이다.

[0229] 수집된 개인정보가 얼마나 오랫동안 보유될 것인지, 그리고 그 정보가 더 이상 필요하지 않을 때 어떻게 파기될 것인지를 정의한다. 이 항목은 정보 보유 기간과 파기 절차를 자동으로 생성하며, 특정 법적 규제(예: GDPR 또는 CCPA)에 맞춘 데이터 보유 및 파기 정책을 포함한다.

[0230] 넷째, 개인정보 위탁 및 제3자 제공이다.

[0231] 개인정보가 외부에 위탁되거나 제3자에게 제공될 경우, 이 과정에서 필요한 모든 법적 절차와 동의서를 관리한다. 개인정보 위탁의 법적 요건, 제3자와의 데이터 공유 방식 등을 명확하게 정의하여 정보주체에게 알리고 동의를 받는다.

[0232] 다섯째, 국외 이전 및 보안 인력이다.

[0233] 개인정보가 국외로 이전되는 경우 그 과정에서 발생하는 보안 요건과 법적 요구사항을 반영한다. 또한, 기업 내 보안 인력의 배치와 그들이 수행하는 역할을 명시하여 데이터 보호 수준을 강화할 수 있도록 설계된다.

[0234] 처리방침 템플릿 반영 자동화 모듈(243)은 생성된 개인정보 처리방침 구성 요소를 템플릿으로 반영하고, 이를 자동화하는 역할을 수행한다. 이 모듈은 사전에 정의된 템플릿에 각 구성 요소를 자동으로 매핑하여 처리방침을 완성한다. 주요 기능은 다음과 같다.

[0235] 첫째, 처리방침 템플릿 관리이다.

[0236] 개인정보 처리방침의 각 항목에 대해 사전 정의된 템플릿을 제공하며, 서비스 제공자의 요구에 맞춰 템플릿을 수정하고 최적화한다. 예를 들어, 금융기관의 경우 더 엄격한 보안 요구 사항을 포함하는 템플릿을 제공하며, 소규모 서비스의 경우 간단한 처리방침을 제공할 수 있다.

[0237] 둘째, 템플릿 자동 매핑이다.

[0238] 서비스 분석 모듈과 처리방침 구성 요소 생성 모듈에서 생성된 데이터를 자동으로 템플릿에 매핑한다. 이 과정은 수작업 없이 처리되며, 각 서비스의 특성에 맞춘 처리방침이 자동으로 생성된다.

[0239] 셋째, 법적 요구 사항 반영이다.

[0240] 템플릿 내에서 법적 요구 사항이 반영되도록 자동화된 규칙을 설정한다. 예를 들어, GDPR이나 CCPA와 같은 규정이 포함된 경우 해당 규정에 맞는 항목이 자동으로 추가되고, 정보주체의 권리와 책임을 명시하는 내용이 포함된다.

[0241] 도 13은 본 개시에 따른 개인정보주체자 토큰 및 동의이력 해시 생성 모듈을 도시한 도면이다.

[0242] 도 13(1310)을 참조하여, 개인정보주체자 토큰 및 동의이력 해시 생성 모듈(250)을 설명한다.

[0243] 개인정보주체자 토큰 및 동의이력 해시 생성 모듈(250)은 B5 모듈(250)에 대응된다.

[0244] 개인정보주체자 토큰 및 동의이력 해시 생성 모듈(250)은 제3자 DID모듈(251), 개인정보주체차 토큰 생성 모듈(252) 및 동의이력 해시 생성 모듈(253)을 포함한다.

[0245] 개인정보주체자 토큰 및 동의이력 해시 생성 모듈(250)은 개인정보 보호 시스템에서 정보주체의 토큰 생성과 동의 이력의 해시(Hash) 값을 생성 및 관리하는 역할을 수행한다. 이 모듈은 정보주체의 인증을 다양한 방식으로 처리하고, 동의 과정에서 발생하는 데이터를 안전하게 저장하며, 해시 값을 통해 기록의 무결성을 유지한다. 또한, 3rd party(DID)와 협력하여 다양한 인증 방식을 제공하고, 정보의 신뢰성을 확보한다.

[0246] 개인정보주체자 토큰 및 동의이력 해시 생성 모듈(250)은 정보주체의 토큰 생성 및 동의 이력 관리에 필요한 모든 절차를 자동화하는 모듈이다. 정보주체의 신원을 안전하게 인증하고, 동의 이력을 해시 값으로 변환하여 무결성을 보장하며, 제출된 개인정보를 철저히 관리하는 이 모듈은 개인정보 보호와 관련된 법적 요구사항을 효과적으로 충족시킬 수 있다

[0247] 도 14는 본 개시에 따른 컴플라이언스 및 보안 위험도 분석부를 도시한 도면이다.

[0248] 도 14(1410)를 참조하여, 컴플라이언스 및 보안 위험도 분석부(300)를 설명한다.

[0249] 컴플라이언스 및 보안 위험도 분석부(300)는 개인정보 위험도 스코어링 모듈(310)을 포함한다.

[0250] 개인정보 위험도 스코어링 모듈(310)은 개인정보 흐름 위험 식별 스코어링 모듈(311), 제3자(수탁사) 협력 스코어링 모듈(312), 개인정보 파기 스코어링 모듈(313), 개인정보 정합성 스코어링 모듈(314), 동의 이력 관리 스코어링 모듈(315), 등록, 처리방침 유지 관리 스코어링 모듈(316) 및 전체 통합 스코어링 모듈(317)을 포함한다.

[0251] 컴플라이언스 및 보안 위험도 분석부(300)는 개인정보 보호 및 컴플라이언스 요구사항을 충족하기 위해 시스템 내에서 개인정보의 위험도를 자동으로 평가하고, 각종 스코어링을 통해 종합적인 위험 평가를 수행한다.

[0252] 컴플라이언스 및 보안 위험도 분석부(300)는 개인정보의 수집, 처리, 보관, 파기 등 모든 단계에서 발생할 수 있는 보안 위험을 평가하여 적절한 보호 조치를 취할 수 있도록 지원한다.

[0253] 컴플라이언스 및 보안 위험도 분석부(300)는 다양한 스코어링 방법을 통해 개인정보의 위험도를 분석하며, 각각의 스코어링은 다음과 같은 기준으로 수행된다.

[0254] 다른 모듈과 연계한 동작 흐름을 설명한다.

[0255] 첫째, 각각의 스코어링이 개별동작한다.

[0256] 둘째, 스코어링 결과에 따라 위험도를 분석한다.

[0257] 개인정보 흐름 위험 식별 스코어링 모듈(311) 개인정보가 수집된 후 시스템 내에서 이동하는 과정에서 발생할 수 있는 위험을 평가한다. 주요 기능은 다음과 같다:

[0258] 첫째, 데이터 이동 경로 분석이다.

[0259] 개인정보가 시스템 내에서 어디로 이동하며, 어떤 방식으로 처리되는지를 추적하고 분석한다. 정보가 이동하는 과정에서 발생할 수 있는 잠재적인 데이터 유출, 권한 없는 접근 등을 식별하여 위험도를 평가한다.

[0260] 둘째, 접근 권한 분석이다.

[0261] 개인정보에 접근할 수 있는 사용자의 권한 수준을 분석하여, 적절한 권한이 부여되었는지 평가한다. 권한이 불필요하게 넓게 설정되었거나, 불법적인 접근 시도가 감지될 경우 위험도가 높게 평가된다.

[0262] 셋째, 데이터 암호화 상태 분석이다.

[0263] 개인정보가 이동하는 동안 적절한 암호화가 적용되었는지 확인한다. 암호화가 적용되지 않거나, 암호화 수준이 낮을 경우 위험도 스코어가 증가한다.

[0264] 제3자(수탁사) 협력 스코어링 모듈(312)은 개인정보가 외부 수탁사나 제3자와 공유될 때 발생하는 위험을 평가하는 모듈이다. 개인정보가 수탁사에 의해 처리될 때 발생할 수 있는 보안 위험을 분석하며, 주요 기능은 다음과 같다:

[0265] 첫째, 수탁사 보안 수준 평가이다.

[0266] 개인정보를 처리하는 수탁사의 보안 정책 및 관리 상태를 평가한다. 수탁사가 적절한 보안 조치를 적용하고 있지 않거나, 보안 인증을 획득하지 못한 경우 위험도가 높게 평가된다.

[0267] 둘째, 데이터 전송 보안 평가이다.

[0268] 개인정보가 제3자에게 전송될 때 사용되는 보안 프로토콜을 분석한다. 예를 들어, 데이터가 암호화된 채로 전송되는지, 보안 인증서가 유효한지를 평가하여 위험도를 산출한다.

[0269] 셋째, 제3자 접근 통제 분석이다.

[0270] 개인정보에 접근할 수 있는 제3자의 권한 및 접근 통제 방법을 분석하여, 불필요한 접근 권한이 부여되었거나 관리가 부실한 경우 위험도가 증가한다.

[0271] 개인정보 파기 스코어링 모듈(313) 수집된 개인정보가 더 이상 필요하지 않거나, 법적 보관 기간이 만료되었을 때 해당 정보를 적절히 파기하는 과정을 평가하는 모듈이다. 주요 기능은 다음과 같다:

[0272] 첫째, 파기 정책 준수 여부 평가이다.

[0273] 개인정보 파기 정책이 관련 법률 및 규제를 준수하는지 평가한다. 예를 들어, GDPR이나 CCPA 등의 법적 요구사항에 따라 개인정보가 적시에 파기되었는지를 확인한다.

[0274] 둘째, 파기 방법 평가이다.

[0275] 개인정보가 적절한 방식으로 완전히 삭제되었는지, 또는 복구 가능성이 있는지 평가한다. 안전한 데이터 삭제 방법(예: 디지털 파쇄, 덮어쓰기 등)이 적용되지 않았을 경우 위험도가 높게 평가된다.

[0276] 셋째, 파기 절차의 투명성 평가이다.

[0277] 파기 과정이 투명하게 관리되고 기록이 남았는지 평가한다. 파기 절차가 불명확하거나 기록이 불완전할 경우, 위험도가 증가한다.

[0278] 개인정보 정합성 스코어링 모듈(314)은 수집된 개인정보가 원래의 목적에 맞게 사용되는지 여부와, 수집된 정보가 정확한지 평가하는 모듈이다. 주요 기능은 다음과 같다:

[0279] 첫째, 수집 목적과의 일치 여부 평가이다.

[0280] 개인정보가 원래 동의받은 목적에 맞게 사용되고 있는지 분석한다. 만약 동의받지 않은 목적으로 개인정보가 사용될 경우, 위험도가 높게 평가된다.

[0281] 둘째, 개인정보의 정확성 평가이다.

[0282] 수집된 개인정보가 정확한지, 잘못된 정보가 입력되었는지 평가한다. 부정확한 정보가 처리되거나, 오류가 발생할 경우 위험도가 증가한다.

[0283] 셋째, 정보주체의 권리 보호 평가이다.

[0284] 정보주체가 자신의 개인정보를 수정, 삭제하거나 그 사용을 중지할 권리를 적절히 행사할 수 있는지 평가한다. 정보주체의 요청이 무시되거나 처리되지 않을 경우 위험도가 높게 평가된다.

[0285] 동의 이력 관리 스코어링 모듈(315)은 개인정보가 수집될 때 정보주체로부터 적절한 동의를 받았는지, 그 동의가 적법하게 관리되고 있는지를 평가하는 모듈이다. 주요 기능은 다음과 같다.

[0286] 첫째, 동의 절차 준수 여부 평가이다.

[0287] 개인정보 수집 및 사용에 대해 정보주체로부터 명확한 동의를 받았는지 평가한다. 적절한 동의 없이 개인정보가 수집되거나 사용된 경우 위험도가 높게 평가된다.

[0288] 둘째, 동의 기록의 관리 상태 평가이다.

[0289] 동의 이력이 안전하게 보관되고, 정보주체의 요청에 따라 동의 철회가 즉시 반영되는지를 평가한다. 동의 기록이 손상되거나 철회 요청이 반영되지 않은 경우 위험도가 증가한다.

[0290] 등록, 처리방침 유지 관리 스코어링 모듈(316)은 개인정보 처리 방침이 적절하게 등록되고 유지되고 있는지 평가하는 모듈이다. 주요 기능은 다음과 같다:

[0291] 첫째, 처리방침의 최신성 평가이다.

[0292] 개인정보 처리방침이 최신 법적 요구사항을 반영하여 지속적으로 업데이트되고 있는지 평가한다. 법적 규정이 변경되었음에도 불구하고 처리방침이 업데이트되지 않았을 경우 위험도가 높게 평가된다.

[0293] 둘째, 처리방침의 투명성 평가이다.

[0294] 정보주체가 처리방침에 쉽게 접근할 수 있으며, 해당 방침이 명확하고 이해하기 쉬운지 평가한다. 처리방침이 불투명하거나 정보주체가 접근하기 어려운 경우 위험도가 증가한다.

[0295] 전체 통합 스코어링 모듈(317)은 각 개별 스코어링 모듈에서 산출된 위험도를 종합하여, 전체적인 개인정보 처리 과정의 통합 위험도를 계산한다. 전체 통합 스코어링은 다음과 같은 요소를 포함한다:

[0296] 첫째, 가중치 적용이다.

[0297] 각 스코어링 모듈의 중요성에 따라 가중치를 적용하여 전체 위험도를 산출한다. 예를 들어, 개인정보 파기 스코어링의 가중치가 높을 경우, 파기 과정의 부실함이 전체 위험도에 큰 영향을 미친다.

[0298] 둘째, 종합 위험도 산출이다.

[0299] 개별 스코어링 결과를 바탕으로 최종 종합 위험도를 계산한다. 종합 위험도는 개인정보 처리의 전반적인 보안 수준을 나타내며, 이에 따라 추가적인 보안 조치나 관리 방안을 제안할 수 있다.

[0300] 도 15는 본 개시에 따른 서비스별 개인정보 분석부를 도시한 도면이다.

[0301] 도 15(1510)를 참조하여, 서비스별 개인정보 분석부(400)를 설명한다.

[0302] 서비스별 개인정보 분석부(400)는 서비스별 개인정보 분석모듈(410)을 포함한다.

[0303] 서비스별 개인정보 분석부(400)는 서비스 제공 중 수집된 개인정보를 가명처리 및 익명처리하여 분석하는 시스템으로, 이를 기반으로 사용자가 제공한 답변 내용을 키워드로 분류하고, 긍정 또는 부정의 의미를 판단하는 역할을 수행한다.

[0304] 서비스별 개인정보 분석부(400) 는 개인정보 보호를 위한 가명화 및 익명화 처리와 함께, 개인정보의 분석을 다양한 단계로 수행하여 서비스 제공에 필요한 기능을 지원한다. 본 발명의 서비스별 개인정보 분석부(400)는 주로 다음과 같은 처리 단계로 구성된다.

[0305] 제 1 단계, 가명처리 단계이다.

[0306] 가명처리 단계는 사용자가 제공한 개인정보에서 특정 개인을 직접 식별할 수 있는 요소를 가명화하여 보호하는 과정이다. 가명처리는 데이터 분석 및 서비스 최적화를 위해 개인정보를 이용하는 동안 개인정보 보호를 강화하는 주요 방식이다. 주요 기능은 다음과 같다.

[0307] 첫째, 개인정보 식별 요소 분리이다.

[0308] 사용자가 제공한 이름, 주민등록번호, 이메일 주소 등의 개인정보는 데이터 분석에 필요한 최소한의 정보로 대체된다. 이를 통해 데이터는 특정 개인을 식별할 수 없는 상태로 처리된다.

[0309] 둘째, 가명화 알고리즘 적용이다.

[0310] 가명처리 과정에서는 랜덤화 또는 해시 함수와 같은 알고리즘을 사용하여 개인정보를 대체한다. 예를 들어, 사용자의 이름을 무작위로 생성된 ID로 대체하여 가명화한다. 이 ID는 동일한 개인을 식별할 수 있으나, 원본 데이터를 직접 추적할 수 없다.

[0311] 셋째, 데이터 분석을 위한 가명 데이터 관리이다.

[0312] 가명처리된 개인정보는 분석 목적에 맞게 관리되며, 원본 데이터와는 분리되어 저장된다. 분석이 끝난 후에는 원본 데이터를 다시 복구하지 않도록 설정할 수 있다.

[0313] 제 2 단계, 익명처리 단계이다.

[0314] 익명처리 단계는 개인정보에서 특정 개인을 식별할 수 있는 모든 요소를 제거하여, 완전히 익명화된 상태로 데이터를 처리하는 과정이다. 익명처리는 개인의 신원을 완전히 알 수 없게 하며, 주로 통계 분석이나 대규모 데이터 분석에서 활용된다. 주요 기능은 다음과 같다.

[0315] 첫째, 개인 식별 요소 완전 제거이다.

[0316] 개인정보에서 이름, 주민등록번호, 주소 등의 식별 가능한 모든 정보를 삭제하거나 대체하여, 데이터 분석 시 특정 개인을 추적할 수 없도록 한다.

[0317] 둘째, 통계적 안전성 강화이다.

[0318] 익명화된 데이터는 개별 정보가 아닌 집계된 데이터로 활용된다. 예를 들어, 사용자의 나이나 성별과 같은 비식별 정보만을 남겨 통계적 분석을 수행한다.

[0319] 셋째, 재식별 방지 조치이다.

[0320] 익명처리된 데이터는 재식별 가능성이 없도록 추가적인 보안 조치가 적용된다. 데이터를 다시 조합하여 원본 데이터를 복원할 수 없도록 다양한 보안 기술이 적용된다.

[0321] 제 3 단계, 질문과 다수의 답변 병합 처리 단계이다.

[0322] 질문과 다수의 답변 병합 처리 단계는 사용자가 제공한 여러 답변을 분석하고 병합하여 일관된 답변을 도출하는 과정이다. 이 과정에서는 여러 답변을 통합하여 최종적인 데이터를 생성하고, 그 데이터를 기반으로 서비스에 적합한 결과를 제공한다. 주요 기능은 다음과 같다.

[0323] 첫째, 질문 분석이다.

[0324] 사용자가 입력한 질문의 내용과 그에 따른 다수의 답변을 분석한다. 자연어 처리(NLP) 기술을 사용하여 질문의 의미를 파악하고, 관련된 답변을 추출하여 처리한다.

[0325] 둘째, 다수 답변 병합이다.

[0326] 다수의 답변이 동일한 질문에 대해 제공된 경우, 중복되거나 모호한 답변을 병합하여 일관된 답변을 도출한다. 이를 통해 답변 데이터의 품질을 높이고, 일관성 있는 결과를 제공한다.

[0327] 셋째, 답변 최적화이다.

[0328] 병합된 답변을 최적화하여, 서비스 제공 시 최적의 답변을 제공할 수 있도록 데이터를 정제한다.

[0329] 제 4 단계, 답변 내용 분석 단계이다.

[0330] 답변 내용 분석 단계는 사용자가 제공한 답변 데이터를 분석하고, 해당 답변의 키워드와 긍정 또는 부정의 의미를 판단하는 과정이다. 이 단계에서는 자연어 처리(NLP) 기술을 활용하여 답변을 분석하고, 주요 키워드를 추출하며, 감성 분석을 통해 답변의 감정을 판단한다. 주요 기능은 다음과 같다.

[0331] 첫째, 키워드 추출이다.

[0332] 사용자가 제공한 답변에서 중요한 키워드를 추출하는 단계이다. 텍스트 데이터에서 자주 등장하거나 문맥상 중요한 단어를 식별하고, 이를 키워드로 분류한다. 예를 들어, "만족", "불만족", "빠르다", "느리다" 등의 키워드를 추출한다.

[0333] 둘째, 긍정 및 부정 판단이다.

[0334] 추출된 키워드를 기반으로 답변이 긍정적인지 부정적인지 자동으로 분류한다. 감성 분석(Sentiment Analysis) 알고리즘을 사용하여, 키워드가 긍정적인 의미를 담고 있는지 부정적인 의미를 담고 있는지 판단한다. 예를 들어, "만족"이라는 키워드는 긍정적인 의미로 분류되고, "불만족"은 부정적인 의미로 분류된다.

[0335] 셋째, 키워드 가중치 부여이다.

[0336] 추출된 키워드에 가중치를 부여하여, 해당 답변이 서비스 제공에 있어 얼마나 중요한지를 판단한다. 중요도에 따라 가중치가 다르게 부여되며, 이를 통해 분석 결과의 정확도를 높인다.

[0337] 답변 내용의 키워드, 긍정, 부정 판단 방법에 대하여 설명한다.

[0338] 첫째, NLP 기반 텍스트 전처리를 수행한다.

[0339] 답변 데이터를 자연어 처리 모델에 입력하여 불필요한 단어를 제거하고, 분석 가능한 형태로 변환한다. 여기에는 토큰화, 불용어 제거, 어간 추출 등의 전처리 작업이 포함된다.

[0340] 둘째, 키워드를 추출한다.

[0341] 전처리된 데이터를 기반으로 중요한 키워드를 추출한다. TF-IDF, Word2Vec 등의 기법을 활용하여 빈도가 높고 문맥에서 중요한 단어를 식별한다.

[0342] 셋째, 감성 분석(Sentiment Analysis)을 수행한다.

[0343] 추출된 키워드를 바탕으로 답변의 감정을 분석하고, 긍정적, 부정적, 중립적 의미를 분류한다. 감성 분석 알고리즘은 사전 학습된 긍정 및 부정 어휘 사전을 사용하여 각 키워드의 감정을 평가한다.

[0344] 넷째, 결과를 도출한다.

[0345] 최종적으로 추출된 키워드와 감성 분석 결과를 결합하여, 답변의 의미를 도출하고 서비스 제공에 필요한 정보를 생성한다.

[0346] 도 16은 본 개시에 따른 개인정보 파기부를 도시한 도면이다.

[0347] 도 16(1610)을 참조하여, 개인정보 파기부(500)에 대하여 설명한다.

[0348] 개인정보 파기부(500)는 개인정보 파기 자동화 및 해시 생성 모듈(510)을 포함한다.

[0349] 개인정보 파기 자동화 및 해시 생성 모듈(510)은 파기이력 해시 생성 모듈(511)을 포함한다.

[0350] 개인정보 파기부(500)는 개인정보의 수집 및 보관 주기가 종료되었을 때 해당 정보를 안전하게 파기하고, 그 과정에서 발생하는 파기 이력을 해시 값으로 생성하여 무결성을 보장하는 시스템이다.

[0351] 개인정보 파기부(500)는 개인정보 파기 절차를 자동화하여, 법적 요구사항을 준수하고 데이터 파기 과정을 투명하게 관리한다. 개인정보 파기부(500)는 다음과 같은 주요 단계로 개인정보를 파기한다.

[0352] 제 1 단계, 개인정보 파기 스케줄러 생성 단계이다.

[0353] 개인정보 파기 스케줄러 생성 단계는 개인정보가 더 이상 보관될 필요가 없을 때, 자동으로 파기 일정을 생성하고 실행하는 단계이다. 이는 개인정보 보유 기간이 종료되었거나, 정보주체의 요청에 따라 즉시 파기가 필요한 경우에 해당한다. 주요 기능은 다음과 같다.

[0354] 첫째, 보유 기간 검토이다.

[0355] 각 개인정보 항목에 대해 보관 기간을 검토하고, 법적 또는 서비스적 요구에 따라 설정된 보관 기간이 초과되었는지를 확인한다. 개인정보는 미리 설정된 보유 기간을 기준으로 검토되며, 초과된 데이터는 파기 대상으로 지정된다.

[0356] 둘째, 파기 일정 자동 설정이다.

[0357] 개인정보가 파기 대상으로 지정되면, 자동으로 파기 스케줄러가 생성되어 파기 일정이 설정된다. 파기 일정은 법적 요구 사항과 시스템 리소스를 고려하여 최적화된 시간에 맞춰 조정될 수 있다.

[0358] 셋째, 즉시 파기 요청 처리이다.

[0359] 정보주체가 개인정보의 즉시 파기를 요청한 경우, 스케줄러는 즉각적으로 파기 일정을 설정하고, 데이터 파기 프로세스를 신속하게 실행한다.

[0360] 제 2 단계, 개인정보 파기 단계이다.

[0361] 개인정보 파기 단계는 스케줄러에 의해 설정된 일정에 따라 개인정보를 실제로 파기하는 과정이다. 이 단계는 물리적 또는 논리적인 방법을 통해 데이터를 안전하게 파기하며, 파기된 정보는 복구할 수 없도록 처리된다. 주요 기능은 다음과 같다:

[0362] 첫째, 논리적 파기이다.

[0363] 시스템 내에서 저장된 개인정보를 삭제하는 방식으로 파기한다. 이를 통해 파일이나 데이터베이스에서 개인정보가 삭제되고, 더 이상 접근하거나 검색할 수 없도록 한다. 논리적 파기는 시스템 내에서 해당 데이터의 인덱스와 참조를 모두 제거함으로써 실행된다.

[0364] 둘째, 물리적 파기이다.

[0365] 물리적 저장 장치에 저장된 개인정보가 포함된 디스크나 기타 저장 매체를 파쇄하거나 삭제하는 방식으로 데이터를 완전히 파기한다. 이 방식은 디스크나 미디어를 물리적으로 파괴하여 데이터를 복구할 수 없도록 처리한다.

[0366] 셋째, 데이터 덮어쓰기이다.

[0367] 논리적으로 삭제된 데이터가 복구되지 않도록, 데이터가 저장된 공간에 무작위 데이터로 여러 차례 덮어쓰기 작업을 수행하여 파기를 확정한다. 이 작업은 디지털 데이터를 완전히 제거하기 위한 안전한 방식으로, 복구 가능성을 차단한다

[0368] 제 3 단계, 파기이력 해시 생성단계이다.

[0369] 파기이력 Hash 생성 단계는 개인정보 파기 후 그 이력을 기록하고, 무결성을 보장하기 위해 해시 값을 생성하는 과정이다. 이 단계에서는 파기된 개인정보와 파기 과정에 대한 정보를 기록하며, 그 정보의 변조를 방지하기 위해 해시 값을 생성한다. 주요 기능은 다음과 같다.

[0370] 첫째, 파기이력 데이터 수집이다.

[0371] 개인정보가 파기된 후, 해당 파기 과정에서 발생한 모든 데이터를 수집한다. 여기에는 개인정보주체 토큰, 인증 방식, 인증일, 수집폼 ID, 동의서 ID, 처리방침 ID 등의 정보가 포함된다. 이러한 데이터는 파기 이력의 신뢰성을 보장하는 중요한 요소이다.

[0372] 둘째, 해시 값 생성이다.

[0373] 수집된 파기이력 데이터를 기반으로 해시 알고리즘(SHA256 등)을 적용하여 고유한 해시 값을 생성한다. 해시 값은 파기 이력의 무결성을 보장하며, 이후 검증 과정에서 데이터를 변조되지 않도록 보호한다.

[0374] 셋째, 파기이력 저장 및 관리이다.

[0375] 생성된 해시 값은 파기된 개인정보의 이력과 함께 안전하게 저장되며, 이후 인증 기관이나 감사 프로세스에서 무결성을 확인할 수 있도록 관리된다. 파기된 데이터의 로그와 해시 값은 외부 접근으로부터 보호되며, 필요 시 데이터 검증을 위해 참조할 수 있다.

[0376] 도 17은 본 개시에 따른 인증 관리부를 도시한 도면이다.

[0377] 도 17(1710)을 참조하여, 인증 관리부(600)를 설명한다.

[0378] 인증관리부(600)는 개인정보보호 인증 관리 모듈(610)을 포함한다.

[0379] 인증 관리부(600)는 개인정보 보호와 관련된 인증을 관리하고 유지하는 시스템으로, 사내에서 발생하는 컴플라이언스 로그를 기반으로 각종 국제 및 국내 표준 인증을 획득하고 유지하는 역할을 수행한다.

[0380] 인증 관리부(600)는 인증 취득 과정에서 발생하는 데이터를 안전하게 처리하고, 인증 기준을 준수하는지 여부를 확인하는 단계로 구성되어 있다. 본 발명의 인증 관리부(600)는 주로 다음과 같은 단계로 인증을 관리한다.

[0381] 제 1 단계, 사내 컴플라이언스 로그 생성 단계이다.

[0382] 사내 컴플라이언스 로그 생성 단계는 시스템 내에서 개인정보 보호 및 관련 법적 규제를 준수하는지 확인하기 위해 발생한 모든 활동을 기록하는 단계이다. 이 로그는 개인정보 처리, 접근 통제, 보안 사고 대응 등과 관련된 데이터를 포함하며, 주로 다음과 같은 정보를 수집하여 저장한다.

[0383] 첫째, 개인정보 처리 활동 기록이다.

[0384] 개인정보 수집, 저장, 처리, 파기와 같은 모든 활동이 사내 컴플라이언스 로그로 기록된다. 각 기록에는 활동의 시점, 담당자, 관련된 정보 등이 포함된다.

[0385] 둘째, 접근 통제 로그이다.

[0386] 개인정보에 접근한 사용자, 권한 수준, 접근 시점 등을 기록하여, 불법적인 접근이나 권한 남용을 예방한다.

[0387] 셋째, 보안 사고 대응 기록이다.

[0388] 개인정보와 관련된 보안 사고가 발생했을 경우, 해당 사고에 대한 대응 내역을 기록한다. 예를 들어, 해킹 시도나 내부에서 발생한 정보 유출 등의 사건 대응 기록이 포함된다.

[0389] 이 단계에서 수집된 로그는 이후 인증 신청 시 필요한 자료로 사용되며, 사내에서 일어나는 모든 개인정보 처리 활동이 투명하게 기록된다.

[0390] 제 2 단계, 사내 컴플라이언스 로그 해시 생성 단계이다.

[0391] 사내 컴플라이언스 로그 해시 생성 단계는 수집된 컴플라이언스 로그 데이터를 무결성을 보장하기 위해 해시 값을 생성하는 단계이다. 해시 값은 데이터를 보호하고, 추후 인증 절차에서 로그의 변조 여부를 검증할 수 있는 중요한 역할을 한다. 주요 기능은 다음과 같다.

[0392] 첫째, 해시 알고리즘 적용이다.

[0393] 수집된 로그 데이터에 SHA256 등과 같은 암호화 해시 알고리즘을 적용하여 고유한 해시 값을 생성한다. 이를 통해 로그 데이터가 변조되지 않았음을 증명할 수 있다.

[0394] 둘째, 로그 무결성 보장이다.

[0395] 생성된 해시 값은 컴플라이언스 로그의 무결성을 보장하며, 이후 인증 기관이 해당 로그를 검토할 때 신뢰성을 제공한다. 이 해시 값은 외부 인증 기관에 제공되어 로그의 정당성을 확인할 수 있도록 지원한다.

[0396] 셋째, 해시 값 저장이다.

[0397] 생성된 해시 값은 안전한 데이터베이스에 저장되며, 이후 인증 절차에서 참조될 수 있다. 저장된 해시 값은 로그 데이터가 변조되지 않았는지 확인할 수 있는 중요한 요소로 사용된다.

[0398] 제 3 단계, 인증 신청 및 관리 단계이다.

[0399] 인증 신청 및 관리 단계는 사내에서 생성된 컴플라이언스 로그와 해시 값을 바탕으로, 국제 및 국내 개인정보 보호 관련 인증을 신청하고 유지하는 단계이다. 주요 인증은 ISO 표준 및 국내외 규제에 따라 관리되며, 해당 인증을 취득하기 위한 절차는 다음과 같다.

[0400] 첫째, ISO 27701이다.

[0401] 개인정보 보호 관리 시스템(PIMS) 인증으로, ISO 27701은 개인정보 보호와 관련된 국제 표준이다. 인증 관리부는 ISO 27701 인증 기준을 준수하는지 여부를 검토하고, 필요한 서류와 로그 데이터를 준비하여 인증 신청을 진행한다. ISO 27701 인증은 개인정보 보호 정책, 리스크 관리, 개인정보 처리 활동 등이 표준에 부합하는지 평가한다.

[0402] 둘째, ISO 27001이다.

[0403] 정보 보안 관리 시스템(ISMS) 인증으로, ISO 27001은 정보 보안과 관련된 국제 표준이다. 이 표준은 정보의 기밀성, 무결성, 가용성을 유지하는 데 필요한 관리 체계를 구축하고 있는지 평가한다. 인증 관리부는 사내 정보 보안 정책과 절차를 ISO 27001 기준에 맞춰 관리하고, 인증을 유지하기 위한 필수 로그 데이터를 생성한다.

[0404] 셋째, ISMS-P이다.

[0405] 국내 개인정보 보호 및 정보 보안 관리 인증으로, ISMS-P는 국내 법적 요구 사항을 준수하는지 평가한다. 이 인증은 정보 보호와 개인정보 보호를 모두 충족하는 관리 체계를 요구하며, 인증 관리부는 ISMS-P 인증을 유지하기 위한 데이터를 수집하고 관리한다.

[0406] 넷째, 기타 인증이다.

[0407] 개인정보 보호 및 정보 보안과 관련된 기타 인증(예: 국가별 개인정보 보호 인증, 산업별 규제 인증 등)도 인증 관리부에서 관리된다. 각 인증의 요구사항에 맞춰 사내 데이터를 관리하고, 필요한 서류 및 자료를 준비하여 인증을 신청한다.

[0408] 이 단계에서, 인증 관리부(600)는 신청 절차부터 인증 유지에 필요한 모든 사항을 관리하며, 인증 기관과의 협력 하에 인증 유지 및 갱신 절차를 지속적으로 수행한다.

[0409] 일 예로, 도 18은 본 개시에 따른 수탁 업체의 현황(1810)을 나타내고 있고, 도 19는 개인 정보 처리 현황(1910)을 나타내고 있고, 도 20은 재 위탁 업체 현황(2010)을 나타내고 있다.

[0410] 도 21은 본 개시에 따른 점검 체크리스트의 점검 항목을 설명한 도면이다.

[0411] 도 21(2110)를 참조하여, 점검 체크리스트의 점검 항목을 설명한다.

[0412] 점검항목은 순서, 영역, 구분, 점검항목, 점검항목 세부내용, 관련 증적, 평가 기준으로 구분된다.

[0413] 영역은 관리적 보호조치를 포함한다.

[0414] 구분은 내부 관리 계획을 포함한다.

[0415] 점검항목은 내부관리 계획 수립 및 시행을 포함한다.

[0416] 관련 증적은 내부 관리계획 전문을 포함한다.

[0417] 평가 기준은 다음과 같다.

[0418] Y - 내부 관리계획 내 필수 사항을 모두 포함하고 있다.

[0419] P - 내부 관리계획 내 일부 사항이 누락되었다.

[0420] N - 내부 관리계획을 수집하지 않았다.

[0421] N/A - 소상공인, 개인 단체 중 1만명 미만의 정보주체에 관하여 개인정보를 처리한다.

[0422] 점검항목 세부내용, 관련 증적, 평가 기준은 다음과 같다.

[0423] 첫째, 제 1 점검항목 세부내용, 관련 증적, 평가 기준이다.

[0424] 질문) 개인정보보호 문서(내부관리계획서 및 관련 규정)에 아래의 사항을 모두 포함하여 수립하고 있습니까.

[0425] 1. 개인정보 보호 조직의 구성 및 운영에 관한 사항

[0426] 2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항

[0427] 3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항

[0428] 4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항

[0429] 5. 접근 권한의 관리에 관한 사항

[0430] 6. 접근 통제에 관한 사항

[0431] 7. 개인정보의 암호화 조치에 관한 사항

[0432] 8. 접속기록 보관 및 점검에 관한 사항

[0433] 9. 악성프로그램 등 방지에 관한 사항

[0434] 10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항

[0435] 11. 물리적 안전조치에 관한 사항

[0436] 12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

[0437] 13. 위험 분석 및 관리에 관한 사항

[0438] 14. 개인정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

[0439] 15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항

[0440] 16. 그 밖에 개인정보 보호를 위하여 필요한 사항"

[0441] 관련 증적은 다음과 같다.

[0442] 1. 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정) 전문

[0443] 평가 기준은 다음과 같다.

[0444] Y - 정책 문서 내 필수 사항을 모두 포함하고 있음

[0445] P - 정책 문서 내 일부 사항이 누락됨

[0446] N - 정책 문서를 수립하지 않음

[0447] N/A - 소상공인·개인·단체 중 1만명 미만의 정보주체에 관하여 개인정보를 처리함

[0448] 둘째, 제 2 점검항목 세부내용, 관련 증적, 평가 기준이다.

[0449] 질문) 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정)을 내부 인사절차에 따라 대표이사(또는 개인정보최고책임자)의 승인을 득하고 있습니까.

[0450] - 그룹웨어(품의) 또는 내부 관리계획 내 승인기록 명시

[0451] 질문) 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정)는 사내 공표하고 있습니까.

[0452] - 그룹웨어 게시판에 내부 관리계획 게시를 통한 공표

[0453] - 소책자 등을 제작하여 열람 가능한 위치에 비치

[0454] 관련 증적은 다음과 같다.

[0455] 1. 승인기록

[0456] 2. 공표 증적

[0457] 평가 기준은 다음과 같다.

[0458] Y - 승인을 득하고 있으며 적절하게 공표하고 있음

[0459] P - 승인을 득하였으나 공표하지 않음

[0460] N - 승인을 득하지 않음

[0461] 셋째, 제 3 점검항목 세부내용이다.

[0462] 질문) 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정)는 정기적(연 1회 이상)으로 검토되고 있습니까.

[0463] - 연 1회 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정)검토 이력

[0464] - 수정 내용에 대한 승인 및 공표 내역

[0465] 관련 증적은 다음과 같다.

[0466] 1. 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정) 수정 이력

[0467] 평가 기준은 다음과 같다.

[0468] Y - 개인정보보호 정책 문서의 수정 이력을 기록하고 있음

[0469] N - 개인정보보호 정책 문서의 수정 이력을 기록하지 않음

[0470] 넷째, 제 4 점검항목 세부내용이다.

[0471] 질문) 개인정보보호 정책 문서(내부관리계획서 및 개인정보보호 관련 규정)의 이행 실태를 연 1회 이상 점검·관리하고 미흡한 사항 등에 대해서 개선조치를 시행하고 있습니까.

[0472] - 개인정보 보호책임자는 연 1회 이상 개인정보보호 정책 문서의 이행 실태 점검 수행

[0473] - 점검 결과에 대한 개인정보 보호책임자의 검토 및 승인

[0474] - 이행 실태 점검 시 필수 점검 사항

[0475] 1. 접근 권한 관리

[0476] 2. 접속기록 보관 및 점검

[0477] 3. 암호화 조치

[0478] 관련 증적은 다음과 같다.

[0479] 1. 개인정보보호 정책의 이행 실태 점검 계획서

[0480] 2. 개인정보보호 정책의 이행 실태 점검 보고서

[0481] 평가 기준은 다음과 같다.

[0482] Y - 개인정보보호 정책의 이행 실태를 연 1회 이상 점검하고 있음

[0483] P - 개인정보보호 정책의 이행 실태를 점검하고 있으나 필수 점검 항목 중 누락된 사항이 있음

[0484] N - 개인정보보호 정책의 이행 실태를 점검하지 않음

[0485] 다섯째, 제 5 점검항목 세부내용이다.

[0486] 질문) 적절한 자격 요건을 갖춘 자로 개인정보 보호책임자를 공식 지정하고 있습니까.

[0487] - 개인정보보호 정책, 조직도, 개인정보 처리방침 내 개인정보 보호책임자 명시

[0488] 1. 사업주 또는 대표자

[0489] 2. 임원(임원이 없는 경우 개인정보 처리 관련 업무를 담당하는 부서의 장)

[0490] ※ 소상공인에 해당하는 경우 별도의 지정 없이 그 사업주 또는 대표자를 개인정보 보호책임자로 지정한 것으로 봄

[0491] 관련 증적은 다음과 같다.

[0492] 개인정보보호 정책, 조직도, 개인정보 처리방침, 인사발령 등 개인정보 보호책임자 지정을 확인할 수 있는 공식적인 문서

[0493] 평가 기준은 다음과 같다.

[0494] Y - 개인정보 보호책임자를 지정하고 개인정보 보호책임자의 지정 요건을 충족함

[0495] P - 개인정보 보호책임자를 지정하고 있으나 개인정보 보호책임자의 지정 요건을 충족하지 않거나 공식문서로 지정되지 않음

[0496] N - 개인정보 보호책임자가 지정되어 있지 않음

[0497] 여섯째, 제 6 점검항목 세부내용이다.

[0498] 질문) 개인정보취급자를 대상으로 개인정보 보호를 위한 보안서약서를 징구하고 있습니까.

[0499] ① 입사 및 퇴사 시 보안서약서 징구 여부 확인

[0500] ② 정기적(연 1회)으로 모든 개인정보취급자를 대상으로 보안서약서 재 징구 여부 확인

[0501] ※ 보안서약서 구성

[0502] - 개인정보를 누출하지 않도록 다음과 같은 책임사항을 환기시킬 수 있는 내용으로 구성함

[0503] 1. 개인정보보호를 위한 개인정보취급자 의무

[0504] 2. 위반 시 징계사항

[0505] 3. 서약서 예시: 개인정보 보안서약서, 비밀유지 서약서 등 관련 증적은 다음과 같다.

[0506] 1. 입사자 보안서약서

[0507] 2. 퇴사자 보안서약서

[0508] 평가 기준은 다음과 같다.

[0509] Y - 보안서약서를 누락 없이 정기적으로 징구하고 있음(연 1회 이상)

[0510] P - 보안서약서를 징구하고 있으나 누락인원이 존재함

[0511] N -보안서약서를 징구하고 있지 않음

[0512] 일곱째, 제 7 점검항목 세부내용이다.

[0513] 질문) 개인정보 보호책임자 및 개인정보취급자를 대상으로 개인정보보호 교육을 연 1회 이상 수행하고 있습니까.

[0514] - 개인정보보호 교육 계획 작성

[0515] ① 아래 내용을 포함한 연간 개인정보보호 교육 계획 작성

[0516] 1. 교육목적 및 대상

[0517] 2. 교육 내용

[0518] 3. 교육 일정 및 방법

[0519] - 개인정보보호 직무별 교육 시행 증적

[0520] ① 개인정보취급자 대상 개인정보보호 교육 시행증적 확인

[0521] ② 연 1회 이상 교육 시행증적 확인

[0522] ③ 교육 미이수자에 대한 관리·감독 여부 확인

[0523] ※ 개인정보취급자: 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자

[0524] 관련 증적은 다음과 같다.

[0525] 1. 개인정보보호 교육 계획서

[0526] 2. 개인정보보호 교육 결과서

[0527] 3. 개인정보보호 교육 자료

[0528] 4. 개인정보보호 교육 이수 확인서

[0529] 5. 개인정보보호 교육 참석자 명단

[0530] 6. 그 외 개인정보보호 교육을 확인할 수 있는 증적

[0531] 평가 기준은 다음과 같다.

[0532] Y - 개인정보보호 교육 계획을 수립하여 연 1회 이상 정기적인 교육을 실시하고 교육 미이수자에 대한 관리감독을 수행하고 있음

[0533] P - 개인정보보호 교육을 연 1회 이상 시행하고 있으나 교육 미이수자에 대한 관리감독을 수행하고 있지 않음

[0534] N - 개인정보보호 교육을 연 1회 이상 시행하고 있지 않음

[0535] 여덟째, 제 8 점검항목 세부내용이다.

[0536] 질문) 개인정보의 분실·도난·유출 등이 발생하는 경우의 대응절차 및 방법을 수립하고 있는가.

[0537] - 유출 신고 및 통지, 피해신고 접수 및 피해 구제 등과 같은 사항을 포함하는 개인정보 유출사고 대응 계획을 수립 및 시행하여야 함

[0538] - 위탁자에게 사고 발생을 즉시 보고하여야 함

[0539] 관련 증적은 다음과 같다.

[0540] 1. 개인정보 유출사고 대응 계획

[0541] 평가 기준은 다음과 같다.

[0542] Y - 개인정보 유출사고 대응 계획을 수립 및 시행하고 있음

[0543] N - 개인정보 유출사고 대응 계획을 수립하지 않음

[0544] 아홉째, 제 9 점검항목 세부내용이다.

[0545] 질문) 사전 협의 없이 수탁자의 재위탁을 원칙적으로 금지하고 있으나 불가피하게 재위탁하는 경우, 기준에 따라 재위탁하고 있습니까.

[0546] - 위탁자의 동의를 받아 재위탁하여야 함

[0547] - 위탁자의 위수탁계약을 기준으로 재위탁 계약서를 작성하여야 함

[0548] - 위탁자로부터 위탁받은 업무 범위를 초과하여 개인정보를 이용하거나 제공할 수 없음

[0549] 관련 증적은 다음과 같다.

[0550] 1. 사전 승인 증적

[0551] 2. 재위탁 관련 계약서

[0552] 평가 기준은 다음과 같다.

[0553] Y - 해당 기준에 따라 개인정보 재위탁을 진행하고 있음

[0554] N - 위탁자의 승인 없이 개인정보를 재위탁하고 있음

[0555] 열번째, 제 10 점검항목 세부내용이다.

[0556] 질문) 개인정보를 재위탁하는 경우, 주기적인 점검 및 교육을 수행하고 있습니까.

[0557] 관련 증적은 다음과 같다.

[0558] 1. 재수탁자 정기적 점검 및 교육 계획

[0559] 2. 재수탁자 정기적 점검 및 교육 결과

[0560] 평가 기준은 다음과 같다.

[0561] Y - 재수탁자에 대한 교육 및 점검을 통해 관리·감독하고 있음

[0562] N - 재수탁자에 대한 교육 및 점검을 통해 관리·감독하고 있지 않음

[0563] N/A - 개인정보를 재위탁하지 않음

[0564] 열한번째, 제 11 점검항목 세부내용이다.

[0565] 질문) 개인정보 처리방침에 아래의 필수 항목을 모두 포함하여 수립하고 정보주체가 알기 쉽게 공개하고 있습니까.

[0566] - 개인정보 처리방침 기재 사항(개인정보 처리방침 작성지침, 개인정보보호위원회, 2024.04.)

[0567] 1. 제목(필수)

[0568] 2. 개인정보의 처리 목적(필수)

[0569] 3. 처리하는 개인정보의 항목(필수)

[0570] 4. 14세 미만 아동의 개인정보 처리에 관한 사항(해당 시 권장)

[0571] 5. 개인정보의 처리 및 보유 기간(필수)

[0572] 6. 개인정보의 파기 절차 및 방법에 관한 사항(필수)

[0573] 7. 개인정보의 제3자 제공에 관한 사항(해당 시 필수)

[0574] 8. 추가적인 이용·제공이 지속적으로 발생 시 판단 기준(해당 시 필수)

[0575] 9. 개인정보 처리업무의 위탁에 관한 사항(해당 시 필수)

[0576] 10. 개인정보의 국외 수집 및 이전에 관한 사항(해당 시 필수)

[0577] 11. 개인정보의 안전성 확보조치에 관한 사항(필수)

[0578] 12. 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당 시 필수)

[0579] 13. 가명정보 처리에 관한 사항(해당 시 필수)

[0580] 14. 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항(해당 시 필수)

[0581] 15. 개인정보 자동 수집 장치를 통해 제3자가 행태정보를 수집하도록 허용하는 경우 그 수집·이용 및 거부에 관한 사항(해당 시 권장)

[0582] 16. 정보주체와 법정대리인의 권리·의무 및 행사방법에 관한 사항(필수)

[0583] 17. 개인정보 보호책임자의 성명 또는 개인정보 업무 담당부서 및 고충사항을 처리하는 부서에 관한 사항(필수)

[0584] 18. 국내대리인 지정에 관한 사항(해당 시 필수)

[0585] 19. 정보주체의 권익침해에 대한 구제방법(권장)

[0586] 20. 고정형 영상정보처리기기 운영·관리에 관한 사항(해당 시 필수)

[0587] 21. 이동형 영상정보처리기기 운영·관리에 관한 사항(해당 시 필수)

[0588] 22. 개인정보처리자가 개인정보 처리 기준 및 보호조치 등에 관하여 자율적으로 개인정보 처리방침에 포함하여 정한 사항(권장)

[0589] 23. 개인정보 처리방침의 변경에 관한 사항(필수)

[0590] - 개인정보 처리방침의 공개

[0591] ① 수립하거나 변경한 개인정보 처리방침은 정보주체가 쉽게 확인 할 수 있도록 운영중인 인터넷 홈페이지에 지속적으로 게재

[0592] ② 인터넷 홈페이지에 게재 할 수 없는 경우 다음과 같은 방법을 통하여 공개

[0593] 1. 개인정보처리자의 사업장 등의 보기 쉬운 장소에 비치

[0594] 2. 연 2회 이상 발행되는 간행물, 소식지, 홍보지 또는 청구서 등에 게재

[0595] 3. 재화나 용역 제공을 위해 정보주체와 작성한 계약서 내 명시 등”

[0596] 관련 증적은 다음과 같다.

[0597] 1. 개인정보 처리방침

[0598] 2. 개인정보 처리방침 공개 증적"

[0599] 평가 기준은 다음과 같다.

[0600] Y - 필수 사항을 모두 포함하여 개인정보 처리방침을 수립하고 지속적으로 공개하고 있음

[0601] P - 개인정보 처리방침 내 필수 사항 중 일부 내용이 누락되어있거나 지속적으로 게재하고 있지 않음

[0602] N - 개인정보 처리방침을 수립하지 않음

[0603] N/A - 개인정보를 재위탁하지 않음"

[0604] 열두번째, 제 12 점검항목 세부내용이다.

[0605] 질문) 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대해 출입통제 절차를 수립 및 운영하고 있습니까.

[0606] - 사무실 출입 통제 절차

[0607] - 지문인식 장치, 카드키 장치, 번호키 장치 등의 추가적인 통제장치 설치"

[0608] 관련 증적은 다음과 같다.

[0609] 1. 출입통제 절차 문서

[0610] 2. 출입통제 적용 현황

[0611] 3. 출입통제 운영 증적(출입대장 등)

[0612] 평가 기준은 다음과 같다.

[0613] Y - 물리적 보관 장소에 대한 출입통제 절차를 수립 및 운영하고 있음

[0614] N - 물리적 보관 장소에 대한 출입통제 절차를 수립하고 있지 않음

[0615] 열세번째, 제 13 점검항목 세부내용이다.

[0616] 질문) 개인정보가 포함된 서류 및 보조저장매체 등을 자료보관실 또는 잠금장치가 있는 안전한 장소에 보관하고 있습니까.

[0617] - 개인정보가 포함된 서류, 보조저장매체를 안전하게 보관

[0618] 관련 증적은 다음과 같다.

[0619] 1. 개인정보가 포함된 서류나 보조저장매체 등을 별도의 공간에 잠금장치로 보관하고 있는 증거자료

[0620] 평가 기준은 다음과 같다.

[0621] Y - 개인정보가 포함된 서류 및 보조저장매체를 안전한 장소에 보관하고 있음

[0622] N - 개인정보가 포함된 서류 및 보조저장매체를 안전한 장소에 보관하고 있지 않음

[0623] 열네번째, 제 14 점검항목 세부내용이다.

[0624] 질문) 보조저장매체의 반출·입 통제 정책을 수립하고 이를 이행하고 있습니까.

[0625] - 내부 규정 내 보조저장매체 외부 반입/반출 절차 수립

[0626] ① 보조저장매체 외부 반입/반출 시 절차 존재 여부 확인

[0627] ② 반입/반출 시 허가 요청 및 승인 절차 존재 여부 확인

[0628] ③ 반입/반출 시 보조저장매체 반출입 관리대장 확인

[0629] 관련 증적은 다음과 같다.

[0630] 1. 보조저장매체 반출입 통제 정책

[0631] 2. 보조저장매체 반출입 관리대장

[0632] 평가 기준은 다음과 같다.

[0633] Y - 보조저장매체 반출입 기준을 수립하고 통제 절차에 따라 이행하고 있음

[0634] P - 보조저장매체 반출입 기준이 미흡하거나 반출입 통제를 하지 않음

[0635] N - 보조저장매체 반출입 기준이 없으며 반출입 통제를 하지 않음

[0636] 열 다섯번째, 제 15 점검항목 세부내용이다.

[0637] 질문) 개인정보처리시스템에 대한 접근권한을 개인정보취급자에게 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있습니까.

[0638] - 개인정보취급자별 계정 발급

[0639] - 계정 공유 금지

[0640] - 부득이하게 계정을 공유하는 경우 책임추적성 확보 조치 필요

[0641] - 개인정보의 출력 및 다운로드 기능 제한

[0642] 관련 증적은 다음과 같다.

[0643] 1. 개인정보취급자 목록

[0644] 2. 개인정보처리시스템 접근권한 현황

[0645] 평가 기준은 다음과 같다.

[0646] Y - 개인정보취급자 계정 권한을 최소한으로 부여하고 있음

[0647] P - 개인정보취급자 계정 권한을 최소한으로 부여하고 있으나 일부 인원에게 과도한 권한이 부여되어 있음

[0648] N - 개인정보취급자 계정의 권한을 제한하지 않음

[0649] 열 여섯번째, 제 16 점검항목 세부내용이다.

[0650] 질문) 전보 또는 퇴직 등 인사이동이 발생하였을 경우 개인정보처리시스템에 대한 접근 권한을 지체없이 변경 또는 삭제하고 있습니까.

[0651] - 업무 변경에 따른 개인정보처리시스템 권한 변경

[0652] - 개인정보처리시스템 내 퇴직자 계정 삭제"

[0653] 관련 증적은 다음과 같다.

[0654] 1. 퇴직 및 직무변경 절차서

[0655] 2. 계정 삭제 또는 접근 권한 변경 이력

[0656] 평가 기준은 다음과 같다.

[0657] Y - 퇴직 등 인사이동 시 접근 권한을 즉시 회수하고 있음

[0658] N - 퇴직 등 인사이동 시 접근 권한을 즉시 회수하지 않음

[0659] 열 일곱번째, 제 17 점검항목 세부내용이다.

[0660] 질문) 개인정보처리시스템에 대한 접근 권한 부여, 변경, 말소에 대한 내역을. 기록하고 해당 기록하고 있습니까.

[0661] - 개인정보처리시스템 접근 권한 변경 내역 최소 3년간 보관

[0662] - 계정명, 성명, 소속, 권한명 등 책임추적성 확보를 위한 최소한의 정보 포함

[0663] 관련 증적은 다음과 같다.

[0664] 1. 개인정보처리시스템 접근 권한 변경 내역

[0665] 2. 접근 권한 변경신청서

[0666] 평가 기준은 다음과 같다.

[0667] Y - 개인정보취급자의 접근 권한 변경 내역을 3년 이상 안전하게 보관함

[0668] P - 개인정보취급자의 접근 권한 변경 내역을 기록하고 있으나 명확하게 변경 이력을 확인할 수 없거나 3년 이상 보관하지 않음

[0669] N - 개인정보취급자의 접근 권한 변경 내역을 기록하지 않음

[0670] 열 여덟번째, 제 18 점검항목 세부내용이다.

[0671] 질문) 개인정보처리시스템으로 일정시간 업무처리를 하지 않는 경우 자동으로 접속이 차단되는 등의 조치를 하고 있습니까.

[0672] - 개인정보처리시스템 세션 타임 아웃, 토큰 만료 시간 설정 등

[0673] 관련 증적은 다음과 같다.

[0674] 1. 최대 접속시간 제한 설정 증적

[0675] 평가 기준은 다음과 같다.

[0676] Y - 개인정보처리시스템 타임아웃 기능이 적용되어 있음

[0677] N - 개인정보처리시스템 타임아웃 기능이 적용되어 있지 않음

[0678] 열 아홉번째, 제 19 점검항목 세부내용이다.

[0679] 질문) 정보통신망을 통해 외부에서 개인 정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하고 있습니까.

[0680] - 안전한 인증수단: OTP, 인증서, 보안토큰 등

[0681] - 안전한 접속수단: VPN, 전용선 등

[0682] 관련 증적은 다음과 같다.

[0683] 1. 외부에서 개인정보처리시스템 접속 시 안전한 인증수단 또는 접속수단을 설정한 증적

[0684] 평가 기준은 다음과 같다.

[0685] Y - 외부에서 개인정보처리시스템으로의 원격 접속을 제한하고 있음

[0686] N - 외부에서 개인정보처리시스템으로의 원격 접속을 제한하지 않음

[0687] 스물번째, 제 20 점검항목 세부내용이다.

[0688] 질문) 개인정보를 처리하는 중요 단말기의 인터넷 접속을 제한하고 있습니까.

[0689] - 아래 업무가 가능한 경우 중요 단말기에 해당함

[0690] 1. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기 가능

[0691] 2. 개인정보처리시스템에 대한 접근 권한 설정 가능

[0692] 관련 증적은 다음과 같다.

[0693] 1. 중요 단말기의 인터넷 차단 설정 증적

[0694] 평가 기준은 다음과 같다.

[0695] Y - 중요 단말기의 인터넷 사용을 제한하고 있음

[0696] N - 중요 단말기의 인터넷 사용을 제한하지 않음

[0697] N/A - 망분리 대상에 해당하지 않음

[0698] 스물 한번째, 제 21 점검항목 세부내용이다.

[0699] 질문) 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하고 있습니까.

[0700] - 방화벽 등을 통해 특정 IP/MAC 접근만 허용

[0701] - 라우터의 ACL 기능을 이용하여 특정 IP/MAC 접근만 허용

[0702] - 접근통제솔루션을 사용하여 허용된 인력의 접근만 허용

[0703] 관련 증적은 다음과 같다.

[0704] 1. 개인정보처리시스템 접속 제한 증적

[0705] 2. 보안솔루션 운영 증적

[0706] 평가 기준은 다음과 같다.

[0707] Y - 개인정보처리시스템 접근 시 접근 통제를 설정하고 있음

[0708] P - 개인정보처리시스템 접근 시 접근 통제가 미흡하게 설정되어 있음

[0709] N - 개인정보처리시스템 접근 시 접근통제를 설정하지 않음

[0710] 스물 두번째, 제 22 점검항목 세부내용이다.

[0711] 질문) 개인정보처리시스템에 대한 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하고 있습니까.

[0712] - 내부 관리계획 또는 지침에 따른 인증수단(비밀번호, OTP 등) 적용

[0713] - 일정 횟수 인증에 실패한 경우 개인정보처리시스템에 대한 접근 제한

[0714] 관련 증적은 다음과 같다.

[0715] 1. 내부 관리계획 내 인증수단 규정

[0716] 2. 인증수단 임계값 설정

[0717] 평가 기준은 다음과 같다.

[0718] Y - 개인정보처리시스템에 대한 인증수단을 적용하고 임계값을 설정하고 있음

[0719] P - 개인정보처리시스템에 대한 인증수단을 적용하고 있으나 임계값을 설정하지 않음

[0720] N - 개인정보처리시스템에 대한 인증수단을 적용하지 않음"

[0721] 스물 세번째, 제 23 점검항목 세부내용이다.

[0722] 질문) 개인정보 조회 또는 출력 시 업무상 필요한 정보로 개인정보 출력 항목을 최소화하고, 출력·복사물을 안전하게 관리하기 위한 안전조치를 적용하고 있습니까.

[0723] - 출력 및 복사물 보호 및 관리 정책/규정/지침 등 마련

[0724] - 워터마킹, 출력 내역 기록, 파기 확인 등 안전조치

[0725] - 개인정보 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하여 접근권한 범위 내에서 최소한으로 출력

[0726] - 개인정보처리시스템을 통한 개인정보 전체 목록 조회 시 마스킹 여부

[0727] 관련 증적은 다음과 같다.

[0728] 1. 개인정보 마스킹 증적

[0729] 평가 기준은 다음과 같다.

[0730] Y - 개인정보 전체 목록 조회 시 안전조치를 적용하고 있음

[0731] N - 개인정보 전체 목록 조회 시 안전조치를 적용하지 않음

[0732] 스물 네번째, 제 24 점검항목 세부내용이다.

[0733] 질문) 개인정보취급자의 개인정보처리시스템에 대한 필수항목을 포함한 접속기록을 1년 이상 보관·관리하고 있습니까.

[0734] - 필수항목 : 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무

[0735] - 아래의 경우 2년 이상 보관·관리하여야 함

[0736] 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우

[0737] 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우

[0738] 3. 개인정보처리자로서 기간통신사업자에 해당하는 경우

[0739] ※ 접속기록 필수항목 설명

[0740] - 식별자 : 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID등 계정정보

[0741] - 접속일시 : 접속한 시간 또는 업무를 수행한 시간(년-월-일, 시:분:초)

[0742] - 접속지 정보: 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등

[0743] - 처리한 정보주체 정보 : 개인정보취급자가 누구의 개인정보를 처리하였는지 알 수 있는 식별정보(ID, 고객번호, 학번, 사번 등)

[0744] - 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보(수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기 등이 수행업무에 해당 될 수 있음)"

[0745] 관련 증적은 다음과 같다.

[0746] 1. 개인정보처리시스템의 접속기록 내역

[0747] 평가 기준은 다음과 같다.

[0748] Y - 개인정보처리시스템의 접속기록을 필수항목을 모두 포함하여 1년 또는 2년 이상 보관·관리하고 있음

[0749] P - 개인정보처리시스템의 접속기록을 보관하고 있으나 일부 정보가 누락되어 있거나 접속기록 보관 기간이 적절하지 않음

[0750] N - 개인정보처리시스템의 접속기록을 보관하지 않음

[0751] 스물 다섯번째, 제 25 점검항목 세부내용이다.

[0752] 질문) 개인정보처리시스템의 접속기록을 월 1회 이상 점검하고 있습니까.

[0753] - 개인정보 과다조회, 근무시간 외 접속, 개인정보 다운로드 사유 등 점검

[0754] - 개인정보 다운로드 시 필수적으로 다운로드 사유를 확인"

[0755] 관련 증적은 다음과 같다.

[0756] 1. 개인정보처리시스템 접속기록 점검 계획

[0757] 2. 개인정보처리시스템 접속기록 점검 보고서

[0758] 평가 기준은 다음과 같다.

[0759] Y - 개인정보처리시스템의 접속기록 및 개인정보 다운로드 사유에 대해 적정성 여부를 점검하고 있음(월 1회 이상)

[0760] P - 개인정보처리시스템 접속기록 및 개인정보 다운로드 사유에 대해 적정성 여부를 점검하고 있으나 월 1회 이상 점검을 실시하지 않음

[0761] N - 개인정보처리시스템의 접속기록 및 개인정보 다운로드 사유에 대해 적정성 여부를 점검하지 않음

[0762] 스물 여섯번째, 제 26 점검항목 세부내용이다.

[0763] 질문) 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 필요한 조치를 하고있습니까.

[0764] - P2P 등 유해 사이트 접속 차단

[0765] - 공유폴더 제한

[0766] - DLP, DRM 등 보안 솔루션 적용

[0767] 관련 증적은 다음과 같다.

[0768] 1. 개인정보취급자 단말기의 유해 사이트 접속 차단 증적

[0769] 2. 공유폴더 제한 설정 증적

[0770] 3. 보안솔루션 운영 증적

[0771] 평가 기준은 다음과 같다.

[0772] Y - 개인정보취급자 단말기에 개인정보 유출 및 노출 방지를 위한 조치를 설정하고 있음

[0773] N - 개인정보취급자 단말기에 개인정보 유출 및 노출 방지를 위한 조치를 설정하지 않음

[0774] 스물 일곱번째, 제 27 점검항목 세부내용이다.

[0775] 질문) 개인정보처리시스템에 접근하는 개인정보취급자 또는 정보주체 계정의 비밀번호 정책을 수립하고 적용하고 있습니까.

[0776] - 비밀번호 최소길이는 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상 조합 시 10자리 또는 3종류 이상 조합 시 8자리 이상의 길이로 설정

[0777] - 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하고, 두개의 비밀번호를 교대로 사용하지 못하도록 설정

[0778] - 비밀번호를 5회 이상 잘못 입력한 경우 계정 잠금, 지연시간 설정 등 접근 제한 조치

[0779] - 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용할 수 없도록 설정

[0780] ※ 인증수단으로 비밀번호를 사용하지 않는 경우 해당 없음"

[0781] 관련 증적은 다음과 같다.

[0782] 1. 내부 관리계획 내 비밀번호 정책

[0783] 2. 개인정보처리시스템에 설정된 비밀번호 정책

[0784] 3. 비밀번호 변경일 현황

[0785] 평가 기준은 다음과 같다.

[0786] Y - 비밀번호 기준에 부합하는 안전한 비밀번호로 설정 및 정기적으로 변경하고 있음

[0787] N - 취약한 비밀번호를 사용하고 있거나 비밀번호 정책 설정이 적용되지 않음

[0788] 스물 여덟번째, 제 28 점검항목 세부내용이다.

[0789] 질문) 비밀번호 저장 시 일방향 암호화하여 저장하고 있습니까.

[0790] - SHA-2 이상의 안전한 일방향 암호 알고리즘 적용

[0791] - KISA 암호 알고리즘 및 키 길이 이용 안내서 등 최신 정보 참고

[0792] ※ 인증수단으로 비밀번호를 사용하지 않는 경우 해당 없음

[0793] 관련 증적은 다음과 같다.

[0794] 1. 비밀번호에 대한 암호화 알고리즘 적용 증적

[0795] 평가 기준은 다음과 같다.

[0796] Y - 비밀번호 저장 시 안전한 암호화 알고리즘을 적용하고 있음

[0797] N - 비밀번호 저장 시 안전한 암호화 알고리즘을 적용하고 있지 않음

[0798] 스물 아홉번째, 제 29 점검항목 세부내용이다.

[0799] 질문) 이용자의 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보는 안전한 암호화 알고리즘으로 암호화하여 저장하고 있습니까.

[0800] - 적용된 대칭키 암호 알고리즘 작성(SEED, ARIA-128/192/256, AES-128/192/256, HIGHT 등)

[0801] - 적용된 공개키 암호 알고리즘 작성(RSAES-OAEP, RSAES-PKCS1 등)"

[0802] 관련 증적은 다음과 같다.

[0803] 1. 개인정보 암호화 적용 증적

[0804] 2. 암호화 알고리즘 증적

[0805] 평가 기준은 다음과 같다.

[0806] Y - 개인정보를 안전한 암호화 알고리즘으로 암호화하여 저장하고 있음

[0807] N - 개인정보를 안전한 암호화 알고리즘으로 암호화하지 않고 저장하고 있음

[0808] 서른번째, 제 30 점검항목 세부내용이다.

[0809] 질문) 정보통신망을 통해 비밀번호, 개인정보 및 인증정보를 송·수신하는 경우 이를 암호화하여 송·수신하고 있습니까.

[0810] - SSL(https) 적용 또는 암호화 프로그램 설치"

[0811] 관련 증적은 다음과 같다.

[0812] 1. SSL 인증서 정보

[0813] 2. 암호화 솔루션 등을 통한 개인정보 암호화 증적

[0814] 평가 기준은 다음과 같다.

[0815] Y - 정보통신망을 통해 송·수신하는 개인정보 및 인증정보를 암호화하고 있음

[0816] N - 정보통신망을 통해 송·수신하는 개인정보 및 인증정보를 암호화하지 않음

[0817] 서른 한번째, 제 31 점검항목 세부내용이다.

[0818] 질문) PC, 모바일 기기 및 보조저장매체 등에 개인정보를 저장하는 경우, 암호화하여 저장하고 있습니까.

[0819] - 개인정보처리시스템으로부터 파일 다운로드 시 암호 설정이 적용된 상태로 다운로드됨

[0820] - 수동으로 개인정보 파일에 암호 설정(오피스 프로그램에서 제공하는 암호 설정 등)

[0821] - 보조저장매체 이용 시 보안 USB 등 활용

[0822] - DRM 적용

[0823] 관련 증적은 다음과 같다.

[0824] 1. PC, 보조저장매체 등 개인정보파일 보관 시 암호화 적용을 확인할 수 있는 증적

[0825] 평가 기준은 다음과 같다.

[0826] Y - 개인정보 저장 시 암호화하여 저장하고 있음

[0827] N - 개인정보 저장 시 암호화하지 않음

[0828] 서른 두번째, 제 32 점검항목 세부내용이다.

[0829] 관련 증적은 다음과 같다.

[0830] 1. 암호 키 관리 절차

[0831] 평가 기준은 다음과 같다.

[0832] Y - 안전한 암호 키 관리 절차를 수립 및 시행하고 있음

[0833] N - 안전한 암호 키 관리 절차를 수립및 시행하지 않음

[0834] 서른 세번째, 제 33 점검항목 세부내용이다.

[0835] 질문) 개인정보취급자 PC에 악성 프로그램을 점검 및 치료하기 위한 보안 프로그램을 설치 및 운영하고 있습니까.

[0836] - 자동 업데이트 또는 일 1회 이상 업데이트

[0837] - 실시간 감시 및 일 1회 예약 검사 실행

[0838] 관련 증적은 다음과 같다.

[0839] 1. 보안 프로그램 설치 내역

[0840] 2. 보안 프로그램 점검 내역

[0841] 3. 보안 프로그램 업데이트 내역

[0842] 평가 기준은 다음과 같다.

[0843] Y - 보안 프로그램을 설치하고 실시간 감시을 실행하고 있으며 일 1회 업데이트를 수행하고 있음

[0844] P - 보안 프로그램을 설치하였으나 일 1회 업데이트를 수행하지 않거나 실시간 감시를 설정하지 않음

[0845] N - 보안 프로그램을 설치 및 운영하지 않음

[0846] 서른 네번째, 제 34 점검항목 세부내용이다.

[0847] 질문) 개인정보취급자 PC에서 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 즉시 업데이트를 적용하고 있습니까.

[0848] 관련 증적은 다음과 같다.

[0849] 1. 개인정보취급자 PC의 보안 업데이트를 확인할 수 있는 화면

[0850] 2. PC에 설치된 응용프로그램의 보안 업데이트를 적용하고 있는지 확인할 수 있는 증거자료

[0851] 3. 업데이트 관련 공지글

[0852] 평가 기준은 다음과 같다.

[0853] Y - 보안 업데이트 공지 시 즉시 업데이트를 적용하고 있음

[0854] N - 보안 업데이트를 즉시 적용하지 않음

[0855] 서른 다섯번째, 제 35 점검항목 세부내용이다.

[0856] 질문) 화재, 홍수, 단전 등 재해·재난 발생을 대비하여 위기대응 매뉴얼과 백업 및 복구 계획을 수립하여 이를 정기적으로 점검하고 있습니까.

[0857] ※ 아래 유형에 해당하는 경우가 아니라면 점검항목에서 제외할 수 있음

[0858] - 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관

[0859] - 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자

[0860] 관련 증적은 다음과 같다.

[0861] 1. 위기대응 매뉴얼(문서)

[0862] 2. 백업 복구 정책 및 절차(문서)

[0863] 평가 기준은 다음과 같다.

[0864] Y - 백업 및 복구 계획 등을 포함한 위기대응 절차를 수립하고 있음

[0865] P - 위기대응 절차를 수립하고 있으나 백업 및 복구 계획이 누락되어 있거나 백업 및 복구 계획은 있으나 위기대응 절차가 미흡함

[0866] N - 위기대응 절차를 수립하지 않음"

[0867] 서른 여섯번째, 제 36 점검항목 세부내용이다.

[0868] 질문) 위탁자로부터 제공받은 개인정보 외에, 위탁자 업무 처리를 위해 개인정보를 추가 수집하는 경우 동의에 필요한 사항을 모두 고지하고 중요한 내용을 표시 하는 등 적절한 방법으로 동의를 받고 있습니까.

[0869] - 동의서 내 고지 필요 내용

[0870] 1. 개인정보의 수집·이용 목적

[0871] 2. 수집하려는 개인정보의 항목

[0872] 3. 개인정보의 보유 및 이용 기간

[0873] 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

[0874] 5. (제3자 제공 시)제공받는 자, 제공받는자의 이용 목적, 이용 기간, 제공받는 항목, 동의거부권과 동의 시 불이익

[0875] - 동의서 내 중요 내용 표시 방법

[0876] 1. 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 표시

[0877] 2. 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용을 명확하게 표시

[0878] 3. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시

[0879] 관련 증적은 다음과 같다.

[0880] 1. 개인정보 수집·이용 동의 화면

[0881] 평가 기준은 다음과 같다.

[0882] Y - 필수 고지 사항을 모두 안내하고 동의를 받아 개인정보를 자체수집하고 있음

[0883] N - 필수 고지 사항을 누락하거나 안내하지 않고 개인정보를 자체수집하고 있음

[0884] 서른 일곱번째, 제 37 점검항목 세부내용이다.

[0885] 질문) 개인정보의 보유기간이 만료되거나 업무목적이 달성된 데이터를 확인하여 지체없이 파기하고 있습니까.

[0886] - 개인정보 파기 조건 및 주기 작성

[0887] - 개인정보 파기 이력 작성

[0888] - '개인정보 파기 확약서' 등 개인정보 파기에 대한 증적 작성요청"

[0889] 관련 증적은 다음과 같다.

[0890] 1. 개인정보 파기 절차서

[0891] 2. 개인정보 파기 배치 설정

[0892] 3. 개인정보 파기 확약서

[0893] 4. 개인정보 파기 이력

[0894] 평가 기준은 다음과 같다.

[0895] Y - 파기 기준 및 절차를 수립하고 파기 후 이력 관리를 하고 있음

[0896] P - 파기 기준 또는 절차를 수립하고 있으나 파기 이력 관리를 하고 있지 않음

[0897] N - 파기 기준 및 절차가 수립되어 있지 않음

[0898] 서른 여덟번째, 제 38 점검항목 세부내용이다.

[0899] 질문) 이용목적 달성 후에도 개인정보를 보관해야 하는 경우, 운영 중인 다른 개인정보와 분리하여 저장 및 관리하고 있습니까.

[0900] - 개인정보 분리보관 조건 및 주기 작성

[0901] 관련 증적은 다음과 같다.

[0902] 1. 개인정보 분리보관 증적

[0903] 평가 기준은 다음과 같다.

[0904] Y - 목적 달성 이후에도 보관이 필요한 개인정보를 운영 중인 개인정보와 분리하여 안전하게 보관하고 있음

[0905] N - 목적 달성 이후에도 보관이 필요한 개인정보를 운영 중인 개인정보와 분리하지 않고 보관하고 있음

[0906] 서른 아홉번째, 제 39 점검항목 세부내용이다.

[0907] 질문) 개인정보는 다음과 같은 안전한 방법으로 파기하고 있습니까.

[0908] - PC, 보조저장매체, 메일함 등 전자적 파일 형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 복구할 수 없는 방법으로 삭제

[0909] - 종이문서로 출력된 개인정보의 경우 쇄절, 소각 등 재생할 수 없는 방법을 이용하여 파기

[0910] 관련 증적은 다음과 같다.

[0911] 1. 전자적 파일 형태로 저장된 개인정보 파기 증거자료

[0912] 2. 문서쇄절기, 문서파기함 증거자료

[0913] 평가 기준은 다음과 같다.

[0914] Y - 개인정보를 안전한 방법으로 파기하고 있음

[0915] N - 개인정보를 파기하고 있지 않음

[0916] 도 22는 본 개시에 따른 점검 체크리스트의 점검 현황을 설명한 도면이다.

[0917] 도 22(2210)를 참조하여 점검 체크리스트의 점검 현황을 설명한다.

[0918] 점검 현황은 점검 현황, 관련 법령, 관련 고시로 구분된다.

[0919] 관련 법령은 개인정보 보호법 제29조, 시행령 제 30조이다.

[0920] 관련 고시는 개인정보의 안전성 확보 조치 기준 제 4조이다.

[0921] 도 23은 본 개시에 따른 점검 체크리스트의 벌칙 규정을 설명한 도면이다.

[0922] 도 23(2310)를 참조하여 점검 체크리스트의 벌칙 규정을 설명한다.

[0923] 벌칙 규정은 벌칙, 벌칙 규정으로 구분된다.

[0924] 벌칙은 형벌, 행정처분으로 구분된다.

[0925] 형벌은 징역, 벌금으로 구분된다.

[0926] 행정처분은 과징금, 과태료로 구분된다. 과태료는 5,000 만원 이하가 될 수 있다.

[0927] 벌칙 규정은 개인정보 보호법 제 75조이다.

[0928] 개인정보 보호법 제75조에 따르면, ①다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

[0929] 5호) 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자이다.

[0930] 이상, 도 1 내지 도 23을 참고하여, 본 개시의 시스템 전체에 대하여 설명하였다. 이하에서는 도 24 내지 도 32를 참고하여, 본 개시에 따른 컴플라이언스 요구 사항 분석 및 점검 자동화 과정에 대해 상세히 설명한다.

[0931] 도 24는 본 개시에 따른 컴플라이언스 요구 사항 분석 및 점검 자동화 장치의 구성도를 도시한 도면이다.

[0932] 도 24를 참조하면, 컴플라이언스 요구 사항 분석 및 점검 자동화 장치(2400)는 입력 모듈(2410), 센서 모듈(2420), 프로세서(2430), 디스플레이 모듈(2440), 메모리(2450), 통신 모듈(2460), 카메라 모듈(2470)를 포함한다.

[0933] 입력 모듈(2410)은 국가별 개인정보의 규제 데이터를 수집한다.

[0934] 센서 모듈 (2420)은 데이터를 센싱한다.

[0935] 프로세서(2430)는 프로세스에 따라 제어 방법을 수행한다.

[0936] 즉, 프로세서(2430)는 국가별 개인정보의 규제 데이터를 입력 모듈(2410)을 통하여 수집하고, 수집된 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습하고, 상기 규제 데이터에 포함된 기업의 계약, 약관, 정책, 지침 및 개인정보 처리방침 중 적어도 하나를 분석하여 상기 기업의 보안 요구사항을 개인정보 라이프사이클 및 보안통제 항목으로 분류하고, 디스플레이(2440)가 상기 개인정보 라이프사이클과 상기 보안통제 항목을 디스플레이하도록 제어하고, 상기 보안 요구사항의 컴플라이언스 준수 여부를 확인하고, 확인 결과를 기초로 위험 평가와 위험 조치 현황을 관리할 수 있다.

[0937] 여기서, 개인정보 라이프사이클은 개인정보의 수집, 이용, 제공, 파기에 이르는 것을 의미한다.

[0938] 여기서, 보안통제 항목은 정책수립, 조직운영(개인정보 교육, 접근권한관리, 접근통제 등), 기술적보호조치(인증수단관리, 개인정보 암호화 등), 정보주체 권리보장 등 개인정보의 수집-이용-제공-파기 이외의 사항을 의미한다.

[0939] 프로세서(2430)는 국가별로 개인정보 보호 규제를 조사하고, 상기 조사한 개인정보 보호 규제를 마이크로 규제 또는 공통 규제로 분류할 수 있다.

[0940] 또한, 프로세서(2430)는 규제 데이터의 크롤링, 업로드, 링크 등록 및 입력 중 적어도 하나를 수행하고, 상기 규제 데이터의 조항별 주요 키워드를 도출하여 개인정보 규제의 태그(tag)를 부여하고, 상기 태그 내용의 유사

도를 계산한다.

[0941] 프로세서(2430)는, 상기 규제 데이터의 업데이트(규제가 추가, 수정, 삭제)가 발생하면, 상기 업데이트된 규제 데이터에 대한 태그를 부여하고, 상기 업데이트된 조항과 기존 조항의 유사도를 계산한다. 이에 대한 자세한 설명은 도 27에서 설명한다.

[0942] 프로세서(2430)는, 하기에서 설명되는 보안 요구사항과 컴플라이언스 및 보안 위험도 분석부(300)에서 분석된 위험도에 대한 결과값을 매핑하고, 상기 결과값이 상기 보안 요구사항의 기준값에 도달했는지를 계산하고, 상기 결과값이 상기 기준값 이상인 경우, 컴플라이언스를 준수하거나 확인이 필요한 사항으로 분류하고, 상기 결과값이 상기 기준값 미만인 경우, 컴플라이언스를 준수하지 않거나 확인이 필요한 사항으로 분류한다.

[0943] 프로세서(2430)는, 확인이 필요한 사항인 경우, 다른 모듈의 결과값을 매핑하여 계산하거나 입력값을 규제 준수 관리자로부터 수신한다. 이에 대한 자세한 설명은 도 29에서 설명한다.

[0944] 프로세서(2430)는, 상기 보안 요구사항과 컴플라이언스 및 보안 위험도 분석부(300)에서 분석된 위험도에 대한 결과값을 매핑하고, 매핑 결과를 기초로 위험도를 계산하고, 상기 디스플레이(2440)가 계산된 상기 위험도를 디스플레이하도록 제어하되, 상기 위험도는 과태료 가능성 및 개인정보 유출위험성 중 적어도 하나를 포함한다.

[0945] 프로세서(2430)는, 상기 위험도에 대응하는 위험 조치를 수행하는 담당자, 기한 및 우선순위를 규제 준수 관리자로부터 수신하고, 위험 조치 사항을 포함하는 메시지를 상기 규제 준수 관리자(또는 상기 담당자)의 디바이스로 전송한다.

[0946] 프로세서(2430)는 위험 조치 트리거가 발생하면, 상태를 위험 조치 완료로 변경하여 위험 수준을 관리한다. 이에 대한 자세한 설명은 도 28에서 설명한다.

[0947] 다만, 도 24에 도시된 구성 요소들은 본 개시에 따른 본 발명을 구현하는데 있어서 필수적인 것은 아니어서, 본 명세서 상에서 설명되는 본 발명은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0948] 한편, 도 24의 프로세서(2430)는 앞서 설명된 도 1의 프로세서(50)와 동일할 수 있고, 이 경우 앞서 설명된 도 1 내지 도 23의 모든 동작 및 제어도 도 24의 프로세서(2440)가 동일하게 수행할 수 있다.

[0949] 디스플레이(2440)는 프로세서(2430)로부터의 제어 명령에 따라 그래픽 이미지를 디스플레이한다.

[0950] 메모리(2450)는 동작의 수행을 위해 적어도 하나의 프로세스가 저장되고 사용자 입력과 데이터를 저장한다.

[0951] 통신 모듈(2460)은 외부 장치와 데이터를 송수신한다.

[0952] 여기서, 상기 외부 장치는 스마트폰, PC, 노트북, 태블릿 PC 등과 같은 외부 디바이스를 포함한다.

[0953] 카메라 모듈(2470)은 전방의 이미지를 캡쳐한다.

[0954] 카메라 모듈(2470)은 프로세서(2430)로부터의 제어 명령에 따라 전방의 피사체를 촬영한다.

[0955] 통신 모듈(2460)은 외부 장치와 통신을 가능하게 하는 하나 이상의 구성 요소를 포함할 수 있으며, 예를 들어, 방송 수신 모듈, 유선통신 모듈, 무선통신 모듈, 근거리 통신 모듈, 위치정보 모듈 중 적어도 하나를 포함할 수 있다.

[0956] 입력 모듈(2410)은 영상 정보(또는 신호), 오디오 정보(또는 신호), 데이터, 또는 사용자로부터 입력되는 정보의 입력을 위한 것으로서, 적어도 하나의 카메라, 적어도 하나의 마이크로폰 및 사용자 입력부 중 적어도 하나를 포함할 수 있다. 입력 모듈(2410)에서 수집한 음성 데이터나 이미지 데이터는 분석되어 사용자의 제어명령으로 처리될 수 있다.

[0957] 디스플레이 모듈(2440)은 본 발명에서 처리되는 정보를 표시(출력)한다. 예를 들어, 본 발명은 구동되는 응용 프로그램(일 예로, 어플리케이션)의 실행화면 정보, 또는 이러한 실행화면 정보에 따른 UI(User Interface), GUI(Graphic User Interface) 정보를 표시할 수 있다.

[0958] 메모리(2450)는 본 발명의 다양한 기능을 지원하는 데이터와, 제어부의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들(예를 들어, 음악 파일, 정지영상, 동영상 등)을 저장할 있고, 다수의 응용 프로그램(application program 또는 애플리케이션(application)), 본 장치의 동작을 위한 데이터들, 명령어들을 저장할 수 있다. 이러한 응용 프로그램 중 적어도 일부는, 무선 통신을 통해 외부 서버로부터 다운로드 될 수 있다.

[0959] 이러한, 메모리(2450)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), SSD 타입(Solid State Disk type), SDD 타입(Silicon Disk Drive type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(random access memory; RAM), SRAM(static random access memory), 롬(read-only memory; ROM), EEPROM(electrically erasable programmable read-only memory), PROM(programmable read-only memory), 자기 메모리, 자기 디스크 및 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 또한, 메모리(2450)는 본 발명과는 분리되어 있으나, 유선 또는 무선으로 연결된 데이터베이스가 될 수도 있으며, 데이터 베이스 시스템으로 구현될 수도 있다.

[0960] 프로세서(2430)는 적어도 하나의 코어를 포함하며, 본 발명 내의 구성요소들의 동작을 제어하기 위한 알고리즘 또는 알고리즘을 재현한 프로그램에 대한 데이터를 저장하는 메모리 및 메모리에 저장된 데이터를 이용하여 전술한 동작을 수행하는 적어도 하나의 프로세서(미도시)로 구현될 수 있다. 이때, 메모리와 프로세서는 각각 별개의 칩으로 구현될 수 있다. 또는, 메모리와 프로세서는 단일 칩으로 구현될 수도 있다.

[0961] 또한, 프로세서(2430)는 이하의 도 24 내지 도 32에서 설명되는 본 개시에 따른 다양한 실시 예들을 구현하기 위하여, 위에서 살펴본 구성 요소들을 중 어느 하나 또는 복수를 조합하여 제어할 수 있다.

[0962] 도 24에 도시된 구성 요소들의 성능에 대응하여 적어도 하나의 구성요소가 추가되거나 삭제될 수 있다. 또한, 구성 요소들의 상호 위치는 시스템의 성능 또는 구조에 대응하여 변경될 수 있다는 것은 당해 기술 분야에서 통상의 지식을 가진 자에게 용이하게 이해될 것이다.

[0963] 한편, 도 24에서 도시된 각각의 구성요소는 소프트웨어 및/또는 Field Programmable Gate Array(FPGA) 및 주문형 반도체(ASIC, Application Specific Integrated Circuit)와 같은 하드웨어 구성요소를 의미한다.

[0964] 도 25는 본 개시에 따른 컴플라이언스 요구 사항 분석 및 점검 자동화 방법의 순서도를 도시한 도면이다. 본 발명은 컴플라이언스 요구 사항 분석 및 점검 자동화 장치(100) 또는 컴플라이언스 요구 사항 분석 및 점검 자동화 장치(2400)의 프로세서(2430)에 의하여 수행된다.

[0965] 프로세서(2430)는 국가별 개인정보의 규제 데이터를 입력 모듈(2410)을 통하여 수집한다(S2510).

[0966] 프로세서(2430)는 수집된 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습한다(S2520).

[0967] 프로세서(2430)는 규제 데이터에 포함된 기업의 약관과 처리 방침을 분석하여 보안 요구사항을 개인정보 라이프사이클과 보안통제 항목으로 분류한다(S2530).

[0968] 프로세서(2430)는 디스플레이(2440)가 상기 개인정보 라이프사이클과 상기 보안통제 항목을 디스플레이하도록 제어한다(S2540).

[0969] 프로세서(2430)는 보안 요구사항의 컴플라이언스 준수 여부를 확인한다 (S2550).

[0970] 프로세서(2430)는 확인 결과를 기초로 위험 평가와 위험 조치 현황을 관리한다 (S2560).

[0971] 도 26은 본 개시에 따른 본 발명의 핵심 개념을 도시한 도면이다.

[0972] 도 26(2610)을 참조하여, 본 발명의 핵심 개념을 설명한다.

[0973] 프로세서(2430)는 기업, 공공기관의 규제 현황을 파악하고, 약관, 처리 방침에서 개인정보 현황을 추출하여 개인정보 라이프사이클에 맞게 분류하여 저장한다.

[0974] 규제종류는 전자상거래, 정보통신망법, 개별법 등이 있고, 규모가 100인 사업장, 규모가 5인 사업장에 따라 다르게 정해진다.

[0975] 또한, 규제는 한국, 미국, 일본, 중국 등 개별 국가에 따라 다르게 정해질 수 있다.

[0976] 프로세서(2430)는 기업, 공공기관의 보안 현황도 상기 내용과 같이 파악하여 진행할 수 있다.

[0977] 본 발명의 프로세서(2430)는 4개의 모듈(2431, 2432, 2433, 2434)을 포함할 수 있다.

[0978] 즉, 프로세서(2430)는 컴플라이언스의 수집, 분석 및 정제를 위한 제1 모듈(2431), 기업정보 처리 현황 및 보안 요구사항의 분석을 자동화하기 위한 제2 모듈(2432), 컴플라이언스의 점검을 위한 제3 모듈(2433), 컴플라이언스의 위험 평가 및 관리를 위한 제4 모듈(2334)를 포함한다.

[0979] 각 모듈의 기능에 대하여 설명한다.

[0980] 첫째, 제1 모듈(2431)은 국가별 개인정보 규제를 수집하고 정책의 tag를 자동 분류 및 재학습하고, 상세 동작은 하기와 같다.

[0981] 1. 국가별 개인정보관련 규제 데이터를 크롤링, 업로드, 링크 등록 및 입력 중 적어도 하나를 수행한다.

[0982] 2. 상기 규제 데이터의 조항별 주요 키워드를 도출하여 각 개인정보 규제에 태그(tag)를 부여하고, 상기 태그 간의 태그 내용의 유사도를 계산한다.

[0983] 3. 상기 규제 데이터의 업데이트가 발생하면, 상기 업데이트된 규제 데이터에 대한 태그를 부여하고, 상기 업데이트된 규제 데이터 내의 업데이트된 조항과 기존 조항의 유사도를 계산한다.

[0984] 4. 국가별로 개인 정보 보호 규제를 조사한다.

[0985] 5. 조사된 개인 정보 보호 규제 별로 tag를 부여한다.

[0986] 6. 부여된 tag를 하나씩 확인하여, 상기 조사한 개인정보 보호 규제를 마이크로 규제 또는 공통 규제로 분류한다.

[0987] 둘째, 제2 모듈(2432)은 기업의 약관과 처리방침을 분석하여 보안요구사항을 개인정보 라이프사이클과 보안통제 항목으로 분류하여 화면에 출력하고, 상세 동작은 하기와 같다.

[0988] 1. 기업의 일반현황과 개인정보 처리현황을 입력 받는다.

[0989] 점검대상의 개인정보처리방침과 이용약관을 등록한다. 구체적으로, 방침과 약관의 내용에서 개인정보 현황을 추출하여 라이프사이클에 맞게 분류하여 저장한다.

[0990] 2. 입력 받은 정보를 바탕으로 컴플라이언스 수집 자동화 모듈(110)에서 유사 tag를 검색한다.

[0991] 3. 결과를 개인정보 라이프사이클과 보안통제 항목으로 분류한다.

[0992] 4. 화면에 출력하여 네비게이션으로 사용한다.

[0993] 셋째, 제3 모듈(133)은 컴플라이언스 준수 여부를 자동으로 점검하고, 상세 동작은 하기와 같다.

[0994] 1. 컴플라이언스 인스펙트 모듈(120)에서 도출된 보안 요구사항을 불러온다.

[0995] 2. 컴플라이언스 및 보안 위험도 분석부(300)의 각 모듈의 결과값을 불러온다.

[0996] 3. 결과값과 요구사항을 맵핑한다.

[0997] 4. 결과값이 요구사항의 기준 값에 도달하였는지를 계산한다.

[0998] 5. 기준 값에 도달하지 않은 경우 준수하지 않거나 확인이 필요한 사항으로 분류한다.

[0999] 6. 기준 값에 도달한 경우 준수하였거나 확인이 필요한 사항으로 분류한다.

[1000] 7. 확인이 필요한 사항은 다른 모듈의 결과값을 맵핑 하여 계산하거나 유저에게 입력 받는다.

[1001] 8. 점검결과를 화면에 출력한다.

[1002] 넷째, 제4 모듈 (2334)은 점검결과를 바탕으로 위험평가와 위험조치 현황을 관리하고, 상세 동작은 하기와 같다.

[1003] 1. 컴플라이언스 인스펙트 모듈(120)에서 도출된 보안 요구사항을 불러온다.

[1004] 2. 회사별 보안 요구사항 분석 자동화 모듈(130)에서 도출된 요구사항별 기준 값 도달 결과를 불러온다.

[1005] 3. 기준 값이 도달하지 않은 경은 요구사항을 위험으로 선정한다.

[1006] 4. 선정된 위험의 수준을 계산한다. 예를 들어, 과태료가능성, 개인정보 유출위험 등의 요소가 될 수 있다.

[1007] 5. 위험 조치를 위한 담당자, 기한, 우선순위 등을 입력 받는다.

[1008] 6. 담당자에게 위험 조치사항을 통보하고 조치 트리거가 발생하기 전까지 주기적으로 반복한다.

[1009] 7. 위험 조치 트리거가 발생하면 조치완료로 상태를 변경하여 위험수준을 관리한다.

[1010] 도 27은 본 개시에 따른 조항별 주요 키워드를 도출하는 실시 예를 도시한 도면이다.

[1011] 도 27(2710)을 참조하여, 조항별 주요 키워드를 도출하는 실시 예를 설명한다.

[1012] 프로세서(2430)는 상기 규제 데이터의 크롤링, 업로드, 링크 등록 및 입력 중 적어도 하나를 수행하고, 상기 규제 데이터의 조항별 주요 키워드를 도출하여 개인정보 규제의 태그(tag)를 부여하고, 상기 태그 내용의 유사도를 계산한다.

[1013] 태그(tag) 생성에 대하여 설명한다.

[1014] 예를 들어, 전자상거래법의 조항이 담고 있는 내용을 기준으로, 해당 조항이 '개인정보' 에 관한 것이고, 라이프사이클에 해당하며, '수집'에 관한 것이면, 프로세서(2430)는 [개인정보], [라이프사이클], [수집] 이라는 태그를 생성한다.

[1015] 예를 들어, 규제 데이터가 전자상거래법인 경우, 프로세서(2430)는 조항별 주요 키워드를 도출한다. 주요 키워드는 통신판매, 통신판매업자, 통신판매중개, 개인정보, 라이프 사이클, 수집을 포함한다.

[1016] 프로세서(2430)는, 상기 규제 데이터의 업데이트(규제의 추가, 수정, 삭제)가 발생하면, 상기 업데이트된 규제 데이터에 대한 태그를 부여하고, 상기 업데이트된 조항과 기존 조항의 유사도를 계산한다.

[1017] 도 28은 본 개시에 따른 보안 요구사항의 컴플라이언스 준수 여부를 확인하는 실시 예를 도시한 도면이다.

[1018] 도 28(2810)을 참조하여, 보안 요구사항의 컴플라이언스 준수 여부를 확인하는 실시 예를 설명한다.

[1019] 프로세서(2430)는 상기 보안 요구사항과 컴플라이언스 및 보안 위험도 분석부(300)에서 분석된 위험도에 대한 결과값을 매핑한다(S2810).

[1020] 프로세서(2430)는 상기 결과값이 상기 보안 요구사항의 기준값에 도달했는지를 계산한다(S2820).

[1021] 프로세서(2430)는 결과값과 기준값을 비교한다(S2830).

[1022] 프로세서(2430)는 상기 결과값이 상기 기준값 미만인 경우, 컴플라이언스를 준수하지 않거나 확인이 필요한 사항으로 분류한다(S2840).

[1023] 프로세서(2430)는 상기 결과값이 상기 기준값 이상인 경우, 컴플라이언스를 준수하거나 확인이 필요한 사항으로 분류한다(S2850).

[1024] 프로세서(2430)는 확인이 필요한 사항인 경우, 다른 모듈의 결과값을 매핑하여 계산하거나 입력값을 규제 준수 관리자로부터 수신한다(S2860).

[1025] 도 29는 본 개시에 따른 위험도를 계산하고 위험 조치를 실행하는 실시 예를 도시한 도면이다.

[1026] 도 29(2910)을 참조하여, 위험도를 계산하고 위험 조치를 실행하는 실시 예를 설명한다.

[1027] 프로세서(2430)는 상기 보안 요구사항과 컴플라이언스 및 보안 위험도 분석부(300)에서 분석된 위험도에 대한 결과값을 매핑한다(S2910).

[1028] 프로세서(2430)는 매핑 결과를 기초로 위험도를 계산한다(S2920).

[1029] 프로세서(2430)는 상기 디스플레이(2440)가 계산된 상기 위험도를 디스플레이하도록 제어한다(S2930).

[1030] 여기서, 위험도는 과태료 가능성 및 개인정보 유출위험성 중 적어도 하나를 포함한다.

[1031] 프로세서(2430)는 상기 위험도에 대응하는 위험 조치를 위한 담당자, 기한 및 우선순위를 규제 준수 관리자로부터 수신한다(S2940).

[1032] 프로세서(2430)는 위험 조치 사항을 포함하는 메시지를 상기 규제 준수 관리자(또는 상기 담당자)의 디바이스로 전송한다(S2950).

[1033] 프로세서(2430)는 위험 조치 트리거가 발생하면, 상태를 위험 조치 완료로 변경하여 위험 수준을 관리한다(S2960).

[1034] 도 30은 본 개시에 따른 종래기술의 문제점을 설명하는 실시 예를 도시한 도면이다.

[1035] 도 30(3010)를 참조하여, 종래기술의 문제점을 설명한다.

[1036] 본 개시의 시스템에 처음 유입되는 사용자들은 자신의 고유의 처리 방침이 있을 수 있다. 그러나 종래기술의 경

우, 도 30(3010)와 같이 잘못된 처리 방침을 업로드해도 아무런 반응이 없어서 사용자가 본인의 처리방침이 맞는 것인지 알 수가 없는 문제점이 있다.

[1037] 종래 기술과 비교한 본원발명의 기술적 특징을 설명한다.

[1038] 종래기술의 경우, pdf 파일만 업로드한다.

[1039] 본원발명의 기술적 특징에 대하여 설명한다.

[1040] 이전 처리 방침을 업로드하면, 해당 처리 방침의 파일을 읽어 해당 피일이 처리방침이 필요한 텍스트를 갖고 있는지 판단하여, 단계에 따라 알려준다.

[1041] 첫째, 처리방침과는 아예 관련이 없는 이상한 파일인 경우이다.

[1042] 해당 파일을 계속 사용할건지 물어보고 아니오 클릭시 삭제한다.

[1043] 둘째, 처리방침이지만 잘못된 처리방침일 경우 설문을 진행한다.

[1044] 셋째, 설문 내용을 토대로 고객의 서비스를 파악하여 처리방침의 내용 중 빠진 내용을 알려주거나 고객의 현재 서비스와 관련이 없는 내용은 제거해야 한다고 알려주고 어떠한 동의서를 작성해야하는지 처리방침 작성페이지에서 어떠한 데이터를 입력해야하는지 알려준다

[1045] 도 31은 본 개시에 따른 처리방침 간단 검토 기능을 설명하는 실시 예를 도시한 도면이다.

[1046] 도 31(3110) 을 참조하여, 처리방침 간단 검토 기능을 설명한다.

[1047] 파일을 업로드한다.

[1048] 첫째, 업로드한 파일이 처리방침이지만 잘못된 파일인 경우이다.

[1049] 1. 설문 조사를 진행한다.

[1050] 2. 설문 내용을 토대로 필요한 동의서 및 처리방침 데이터를 알려준다.

[1051] 둘째, 업로드한 파일이 완전히 잘못된 파일인 경우이다.

[1052] 1. 잘못된 파일이나 사용하지 않는 것을 권장하는 경고장을 알려준다.

[1053] 2. 본 발명의 시스템을 통해 동의서 및 처리 방법을 작성하도록 유도한다.

[1054] 셋째, 업로드한 파일이 잘 작성된 처리 방침 파일인 경우이다.

[1055] 1. 본 발명의 시스템을 사용하면, 지속적으로 이력관리와 수정이 편한 것과 같은 장점을 알려주어 유료 결제를 유도한다.

[1056] 도 32는 본 개시에 따른 처리방침 간단 검토 방법의 순서도를 도시한 도면이다.

[1057] 도 32를 참조하여, 처리방침 간단 검토 방법의 순서도를 설명한다.

[1058] 본 발명은 Front(단말, 3220), Back(서버, 3210), 스토리지 서버(3230)를 포함한다.

[1059] 파일 업로드 클릭 버튼을 사용자로부터 수신하면, 단말(3220)은 파일을 서버(3210)로 업로드한다.

[1060] 서버(3210)는 파일을 스토리지 서버(3230)로 전송한다.

[1061] 스토리지 서버(3230)는 파일을 서버(3210)로 전송한다.

[1062] 서버(3210)는 파일을 분석하고 분서값을 단말(3220)로 전송한다.

[1063] 단말(3220)을 파일 분석값을 화면에 디스플레이한다. 이 경우, 파일 분석값에 따라 3가지 경우의 수로 화면에 표현될 수 있다.

[1064] 단말(3220)은 설문 조사값을 서버(3210)로 전송한다.

[1065] 서버(3210)는 필요 동의서와 처리방침 데이터를 단말(3220)로 전송한다.

[1066] 단말(3220)은 동의서 생성 페이지로 이동 후 동의서 생성부터 처리방침 작성까지 가이드를 화면에 표시한다.

[1067] 본 개시의 다양한 실시 예는 모든 가능한 조합을 나열한 것이 아니고 본 개시의 대표적인 양상을 설명하기 위한

것이며, 다양한 실시 예에서 설명하는 사항들은 독립적으로 적용되거나 또는 둘 이상의 조합으로 적용될 수도 있다.

[1068] 상기 전술한 프로그램은, 상기 컴퓨터가 프로그램을 읽어 들여 프로그램으로 구현된 상기 방법들을 실행시키기 위하여, 상기 컴퓨터의 프로세서(CPU)가 상기 컴퓨터의 장치 인터페이스를 통해 읽힐 수 있는 C, C++, JAVA, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다. 이러한 코드는 상기 방법들을 실행하는데에 필요한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Functional Code)를 포함할 수 있고, 상기 기능들을 상기 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수 있다. 또한, 이러한 코드는 상기 기능들을 상기 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 상기 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조되어야 하는지에 대한 메모리 참조관련 코드를 더 포함할 수 있다. 또한, 상기 컴퓨터의 프로세서가 상기 기능들을 실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 상기 컴퓨터의 통신모듈을 이용하여 원격에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수 있다.

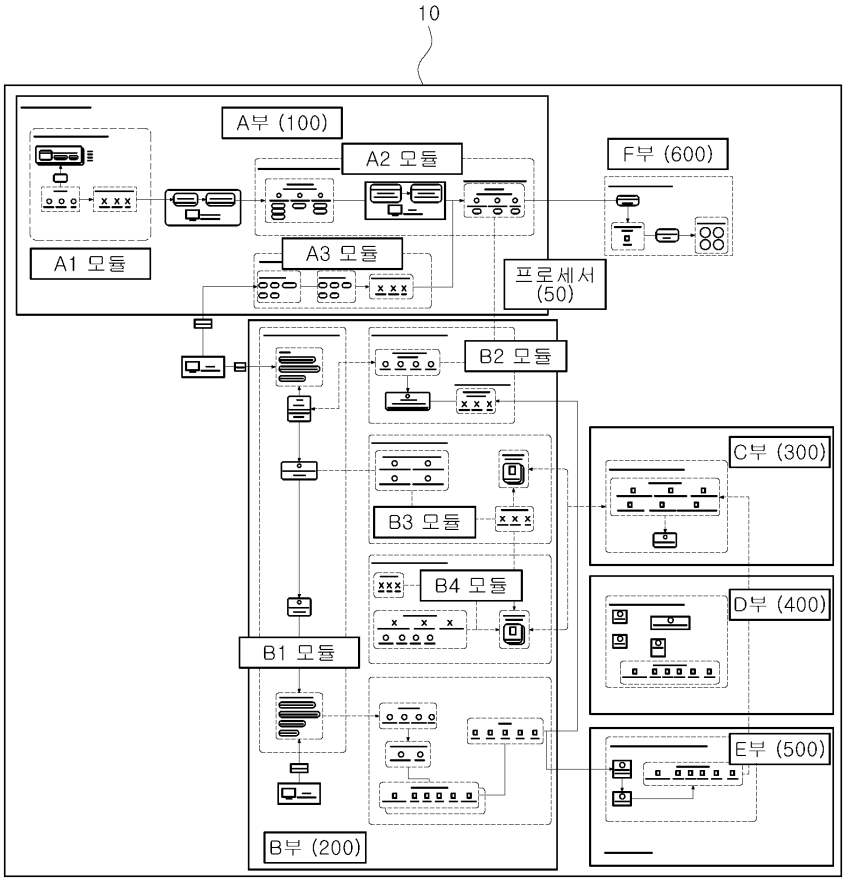
[1069] 상기 저장되는 매체는, 레지스터, 캐쉬, 메모리 등과 같이 짧은 순간 동안 데이터를 저장하는 매체가 아니라 반영구적으로 데이터를 저장하며, 기기에 의해 판독(reading)이 가능한 매체를 의미한다. 구체적으로는, 상기 저장되는 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있지만, 이에 제한되지 않는다. 즉, 상기 프로그램은 상기 컴퓨터가 접속할 수 있는 다양한 서버 상의 다양한 기록매체 또는 사용자의 상기 컴퓨터상의 다양한 기록매체에 저장될 수 있다. 또한, 상기 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장될 수 있다.

[1070] 본 개시의 실시예와 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 개시가 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 판독가능 기록매체에 상주할 수도 있다.

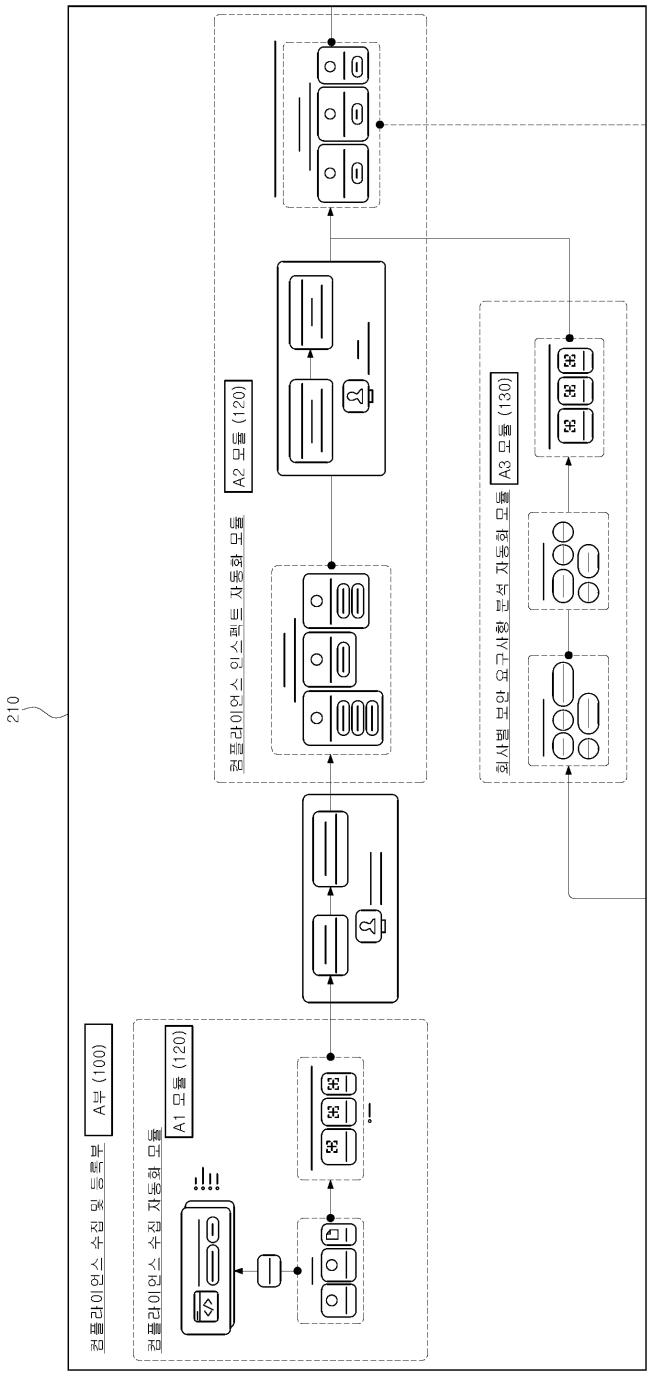
[1071] 이상, 첨부된 도면을 참조로 하여 본 개시의 실시예를 설명하였지만, 본 개시가 속하는 기술분야의 통상의 기술자는 본 개시가 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.

도면

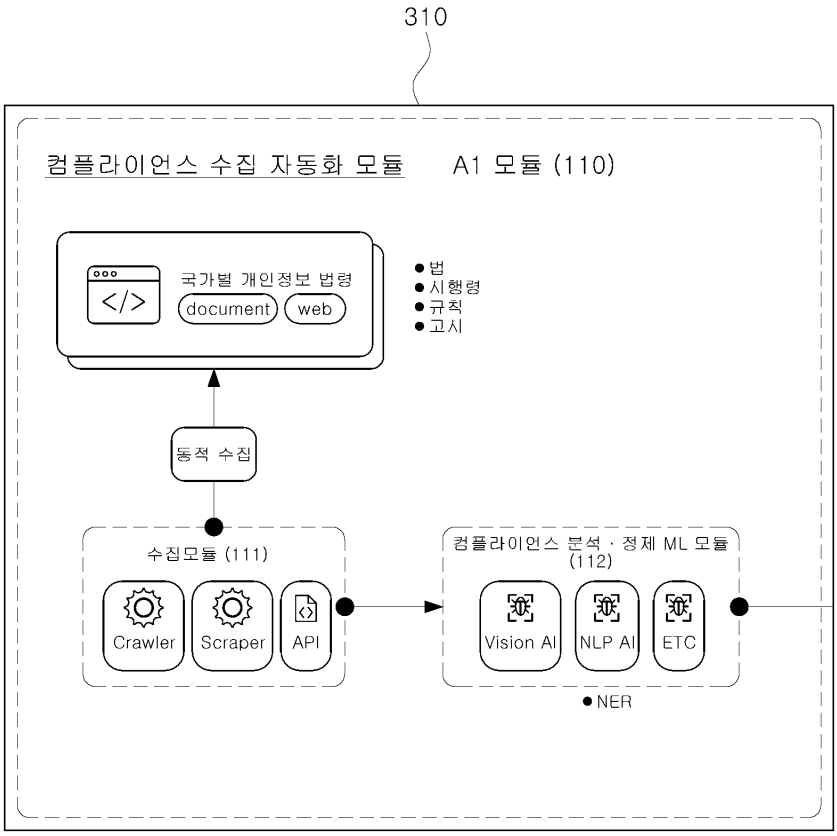
도면1


10
A부 (100)
A2 모듈
F부 (600)
A1 모듈
A3 모듈
프로세서
(50)
B2 모듈
C부 (300)
B3 모듈
B4 모듈
D부 (400)
B1 모듈
E부 (500)
B부 (200)

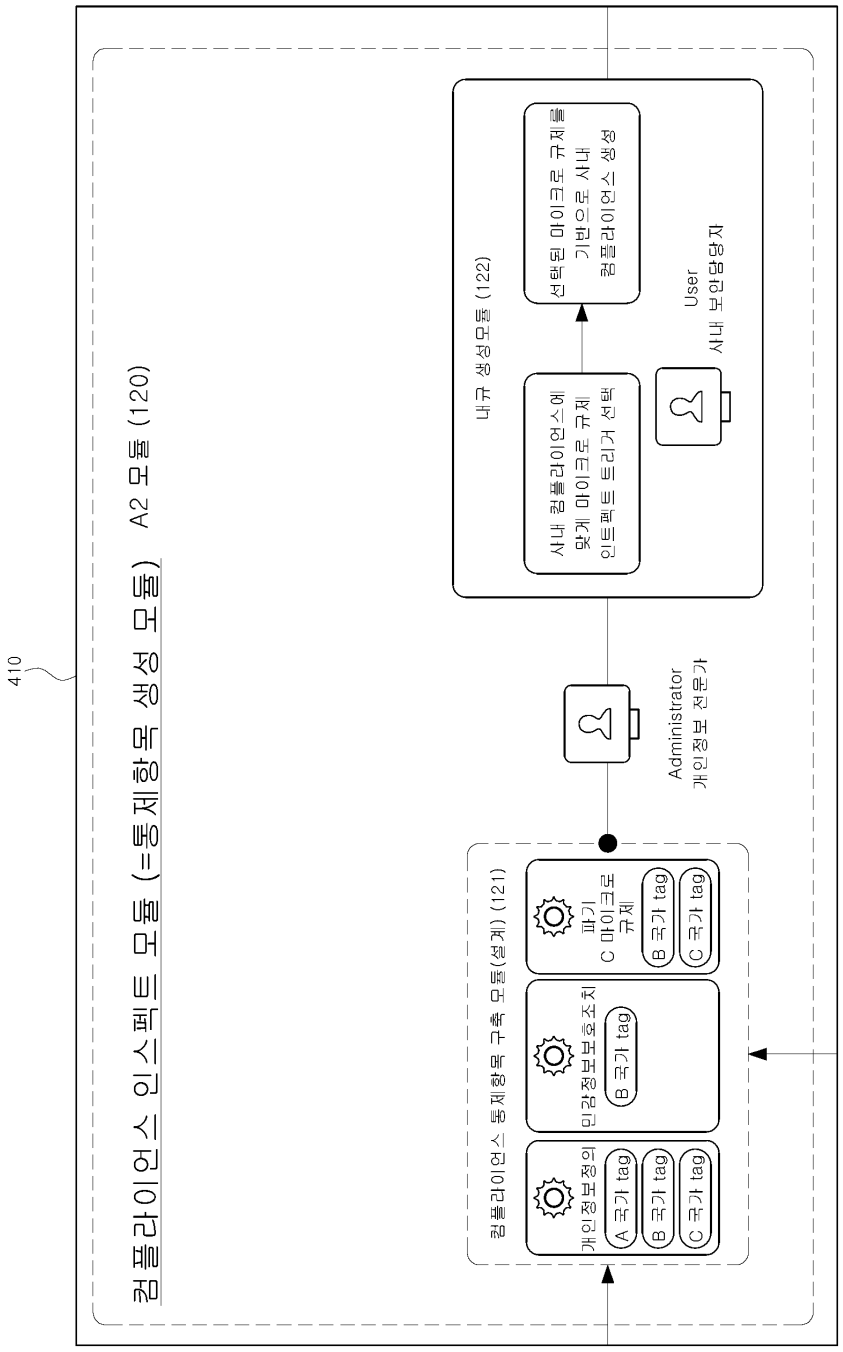
도면2


210
컴플라이언스 수집 및 등록부 A부 (100)
컴플라이언스 수집 자동화 모듈 A1 모듈 (120)
컴플라이언스 인스펙트 자동화 모듈 A2 모듈 (120)
회사별 보안 요구사항 분석 자동화 모듈 A3 모듈 (130)

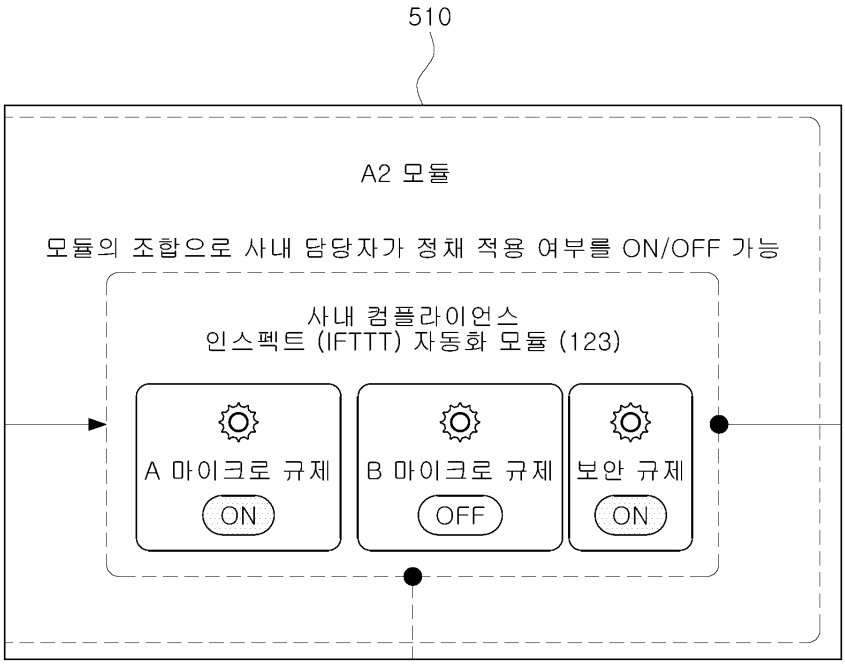
도면3


310
컴플라이언스 수집 자동화 모듈
A1 모듈 (110)
국가별 개인정보 법령
document
web
● 법
● 시행령
● 규칙
● 고시
동적 수집
수집모듈 (111)
Crawler
Scraper
API
컴플라이언스 분석 · 정제 ML 모듈 (112)
Vision AI
NLP AI
ETC
● NER

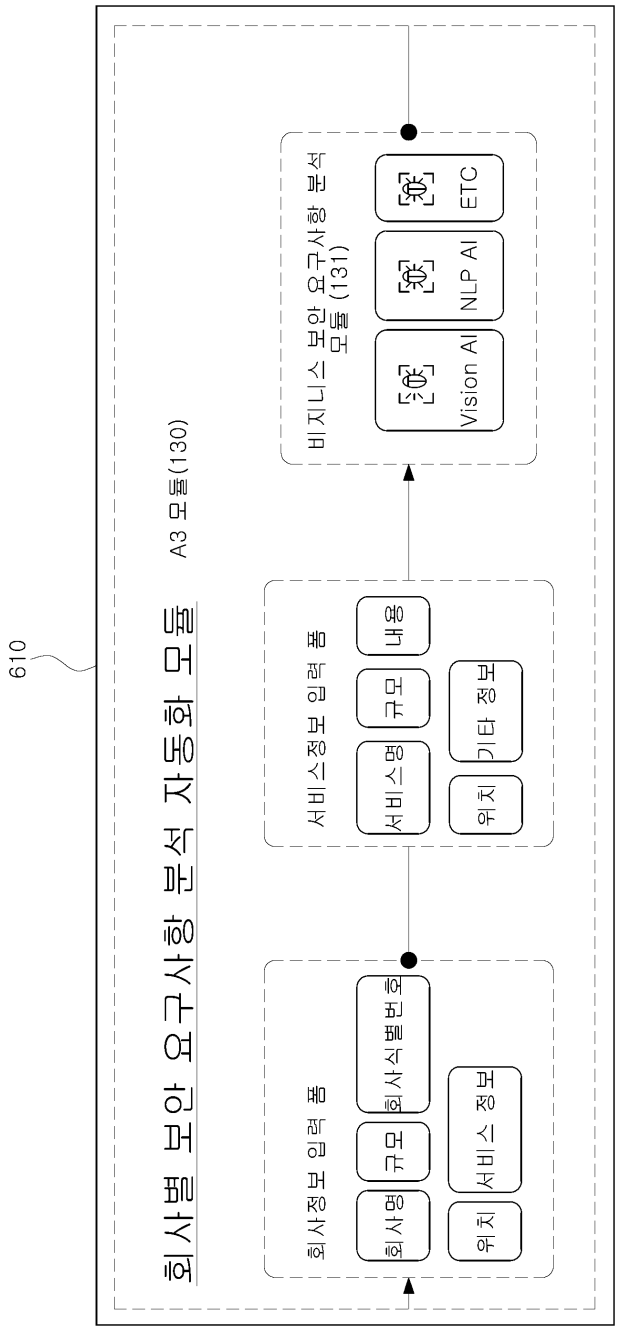
도면4


410
컴플라이언스 인스펙트 모듈 (=통제항목 생성 모듈) A2 모듈 (120)
컴플라이언스 통제항목 구축 모듈(설계) (121)
개인정보보장의
A 국가 tag
B 국가 tag
C 국가 tag
민감정보보호조치
B 국가 tag
파기
C 마이크로 규제
B 국가 tag
C 국가 tag
Administrator
개인정보 전문가
내규 생성모듈 (122)
사내 컴플라이언스에 맞게 마이크로 규제 인트펙트 트리거 선택
선택된 마이크로 규제를 기반으로 사내 컴플라이언스 생성
User
사내 보안담당자

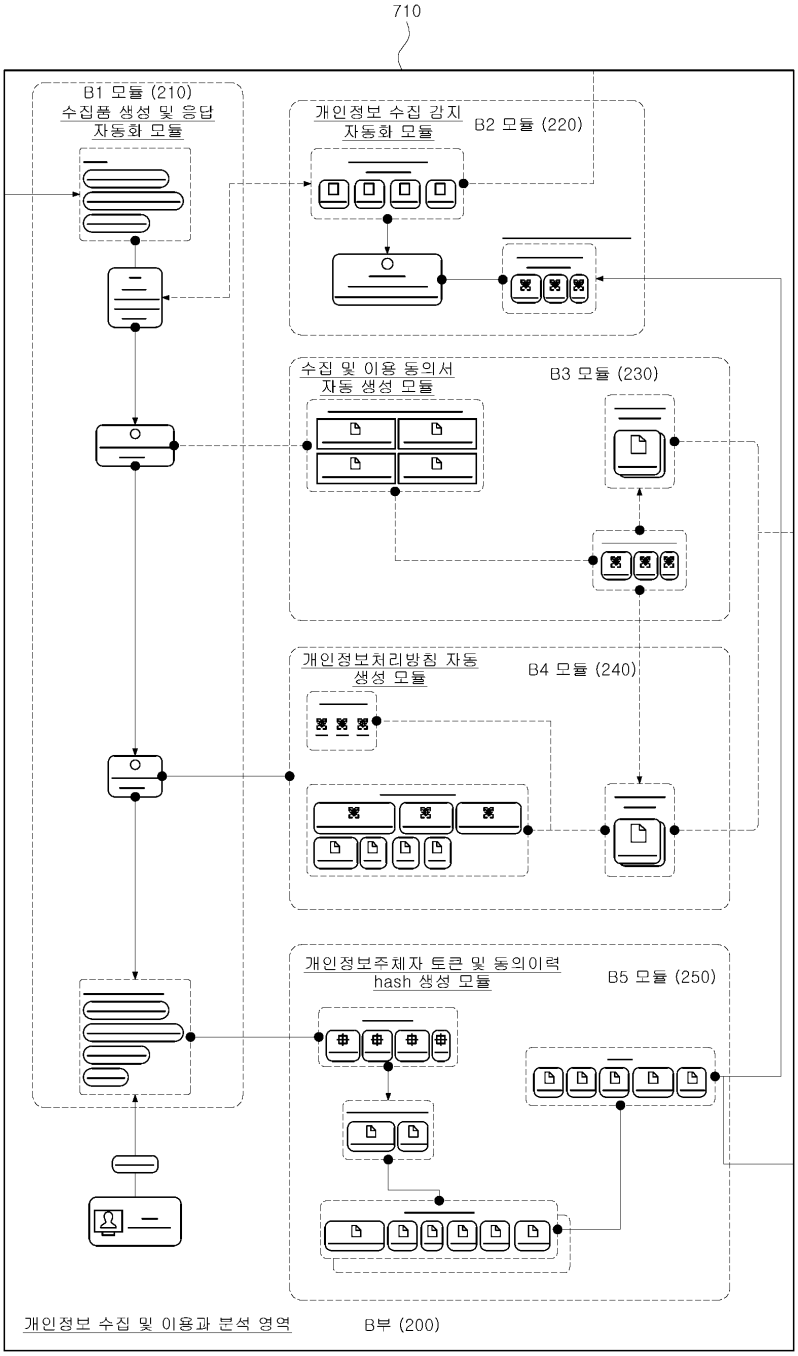
도면5


510
A2 모듈
모듈의 조합으로 사내 담당자가 정책 적용 여부를 ON/OFF 가능
사내 컴플라이언스
인스펙트 (IFTTT) 자동화 모듈 (123)
A 마이크로 규제
ON
B 마이크로 규제
OFF
보안 규제
ON

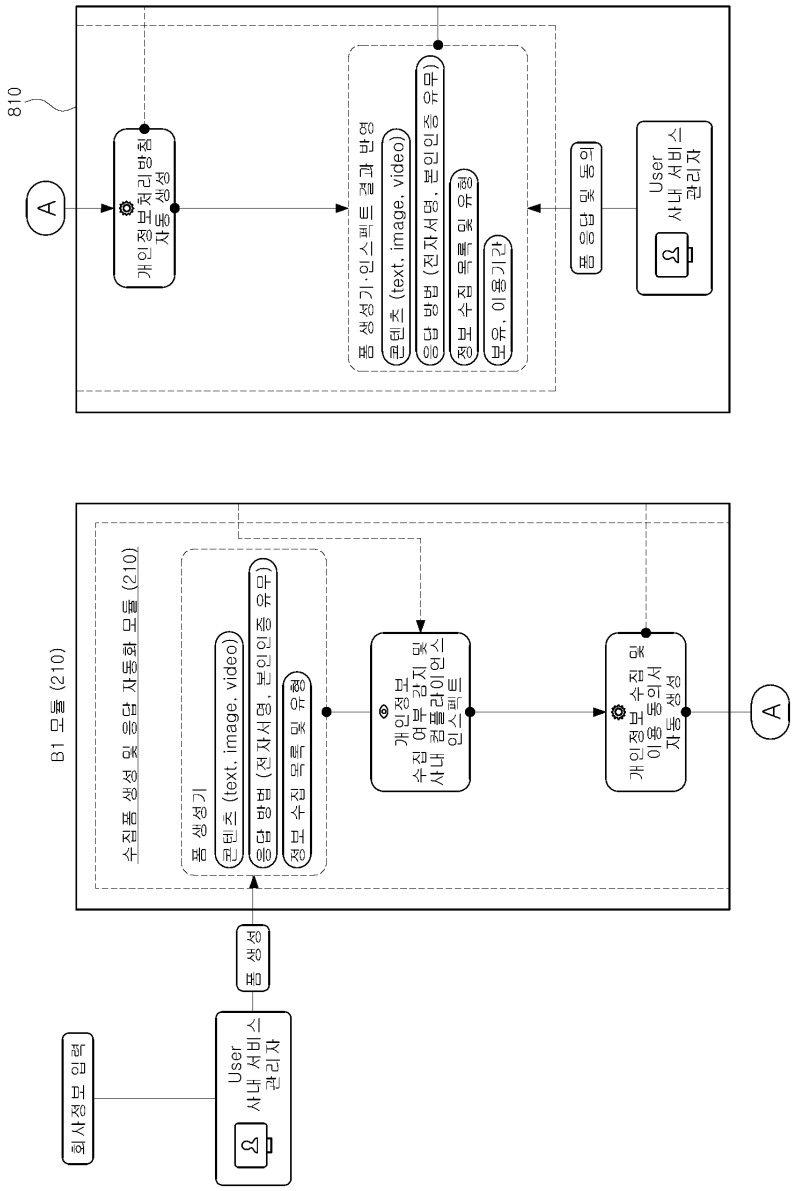
도면6


610
회사별 보안 요구사항 분석 자동화 모듈
A3 모듈(130)
회사정보 입력 폼
회사명
규모
회사식별번호
위치
서비스 정보
서비스정보 입력 폼
서비스명
규모
내용
위치
기타 정보
비지니스 보안 요구사항 분석 모듈 (131)
Vision AI
NLP AI
ETC

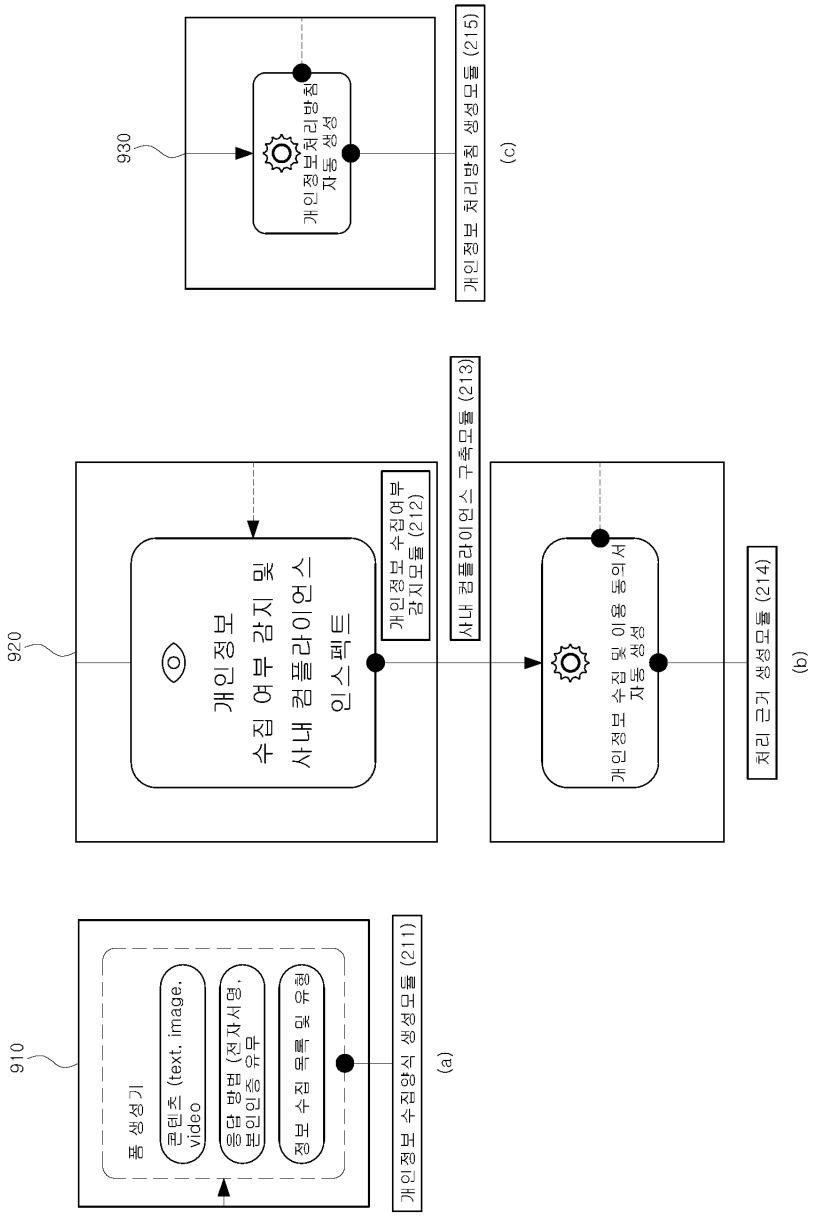
도면7


710
B1 모듈 (210)
수집품 생성 및 응답
자동화 모듈
개인정보 수집 감지
자동화 모듈
B2 모듈 (220)
수집 및 이용 동의서
자동 생성 모듈
B3 모듈 (230)
개인정보처리방침 자동
생성 모듈
B4 모듈 (240)
개인정보주체자 토큰 및 동의이력
hash 생성 모듈
B5 모듈 (250)
개인정보 수집 및 이용과 분석 영역
B부 (200)

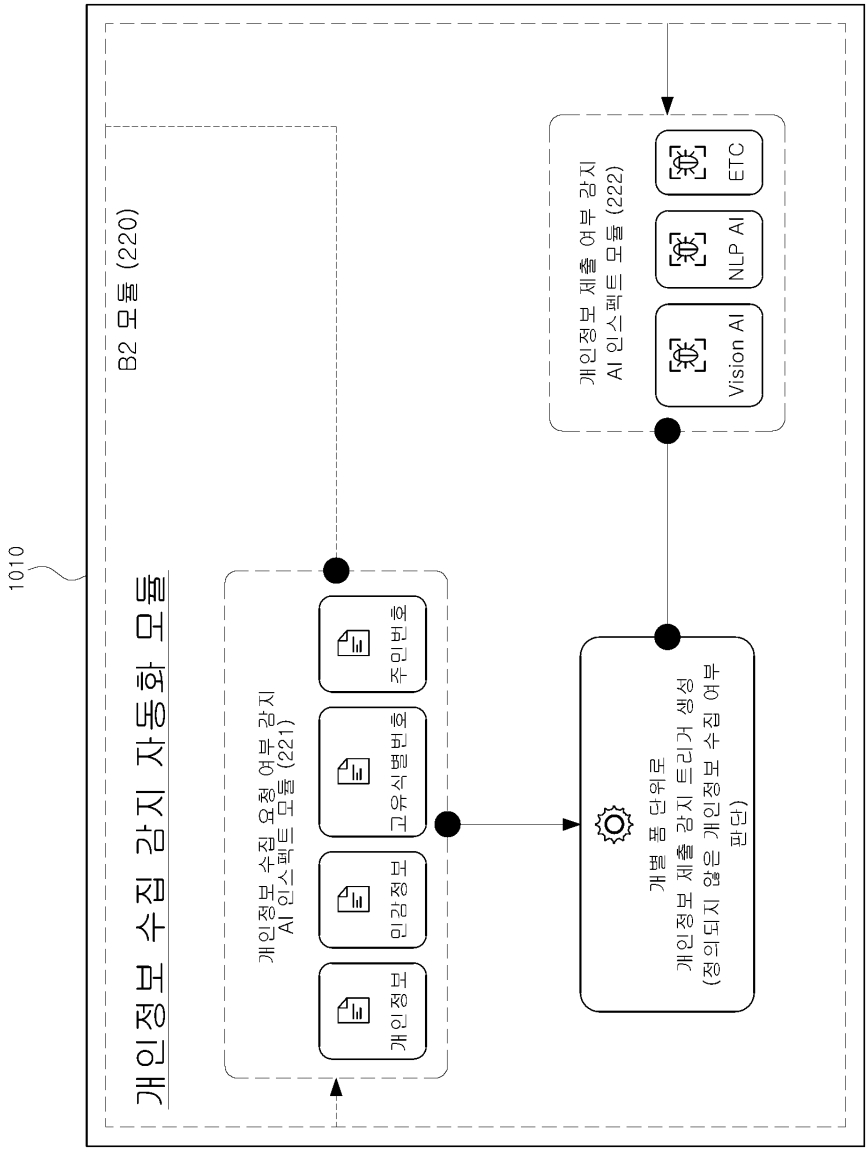
도면8


810
A
개인정보처리방침
자동 생성
폼 생성기·인스펙트 결과 반영
콘텐츠 (text, image, video)
응답 방법 (전자서명, 본인인증 유무)
정보 수집 목록 및 유형
보유, 이용기간
폼 응답 및 동의
User
사내 서비스
관리자
B1 모듈 (210)
수집품 생성 및 응답 자동화 모듈 (210)
폼 생성기
콘텐츠 (text, image, video)
응답 방법 (전자서명, 본인인증 유무)
정보 수집 목록 및 유형
개인정보
수집 여부 감지 및
사내 컴플라이언스
인스펠트
개인정보 수집 및
이용 동의서
자동 생성
A
폼 생성
User
사내 서비스
관리자
회사정보 입력

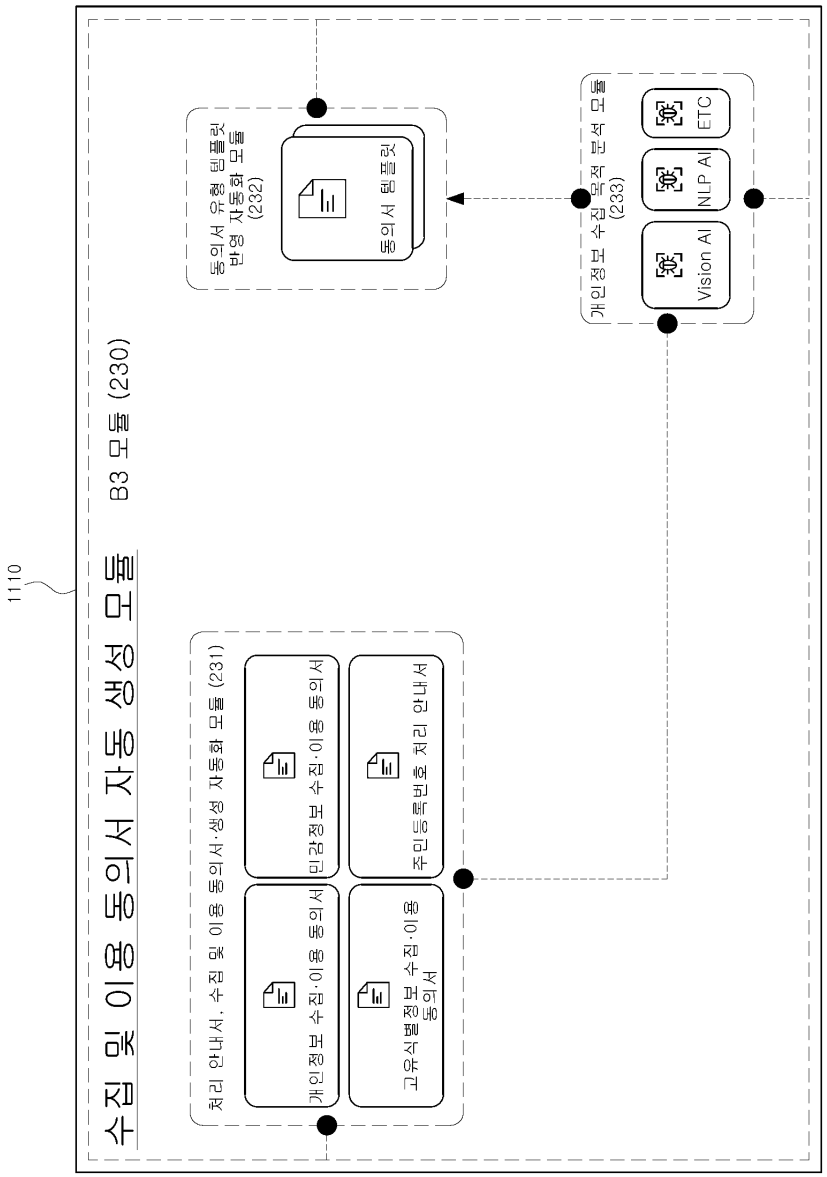
도면9


910
폼 생성기
콘텐츠 (text, image, video
응답 방법 (전자서명, 본인인증) 유무
정보 수집 목록 및 유형
개인정보 수집양식 생성모듈 (211)
(a)
920
개인정보
수집 여부 감지 및
사내 컴플라이언스
인스펙트
개인정보 수집여부 감지모듈 (212)
사내 컴플라이언스 구축모듈 (213)
개인정보 수집 및 이용 동의서 자동 생성
처리 근거 생성모듈 (214)
(b)
930
개인정보처리방침 자동 생성
개인정보 처리방침 생성모듈 (215)
(c)

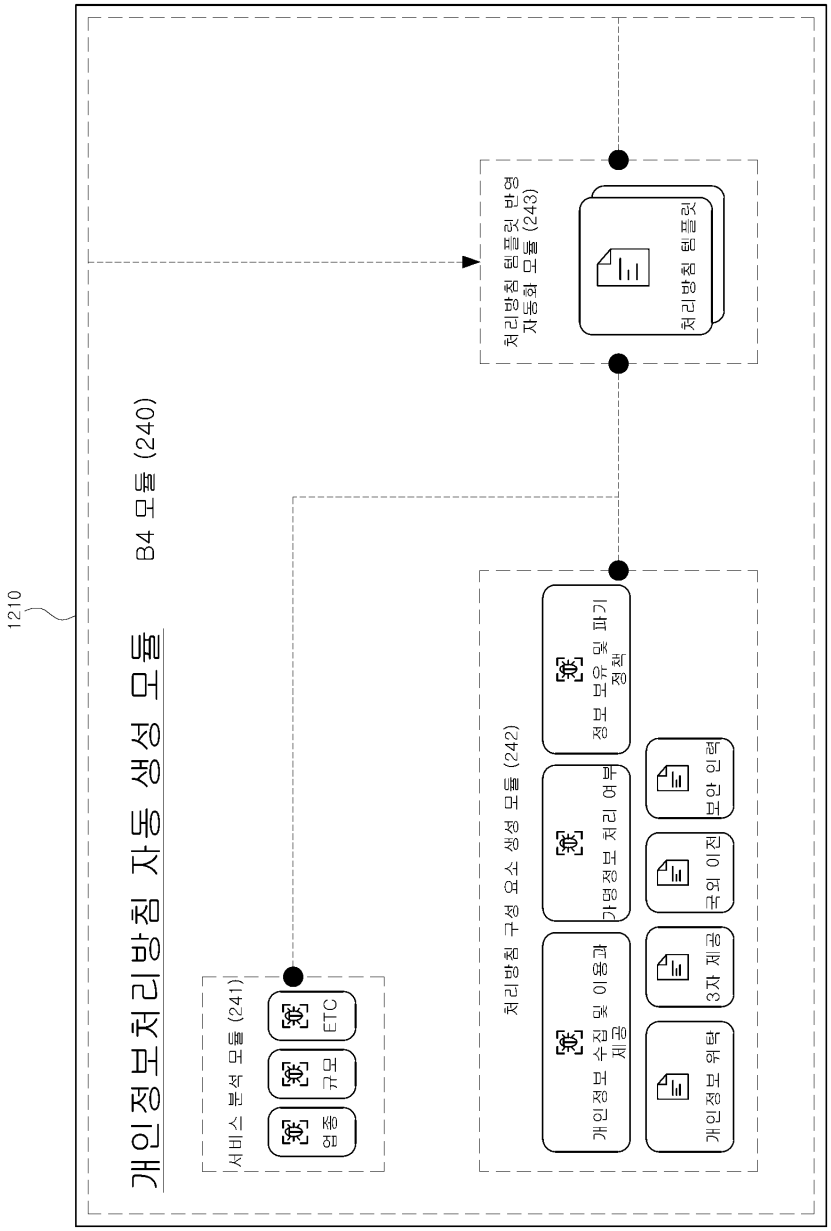
도면10


1010
개인정보 수집 감지 자동화 모듈
B2 모듈 (220)
개인정보 수집 요청 여부 감지
AI 인스펙트 모듈 (221)
개인정보
민감정보
고유식별번호
주민번호
개별 폼 단위로
개인정보 제출 감지 트리거 생성
(정의되지 않은 개인정보 수집 여부
판단)
개인정보 제출 여부 감지
AI 인스펙트 모듈 (222)
Vision AI
NLP AI
ETC

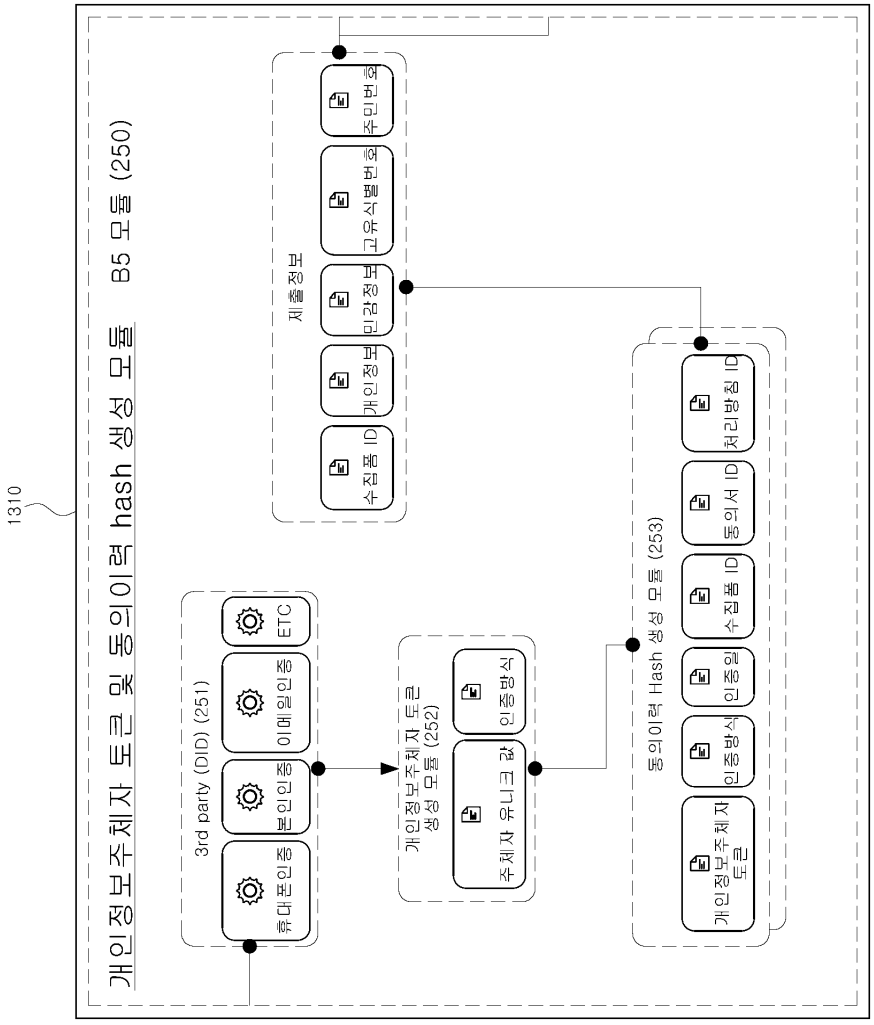
도면11


1110
수집 및 이용 동의서 자동 생성 모듈 B3 모듈 (230)
처리 안내서, 수집 및 이용 동의서·생성 자동화 모듈 (231)
개인정보 수집·이용 동의서
민감정보 수집·이용 동의서
고유식별정보 수집·이용 동의서
주민등록번호 처리 안내서
동의서 유형 템플릿 반영 자동화 모듈 (232)
동의서 템플릿
개인정보 수집 및 분석 모듈 (233)
Vision AI
NLP AI
ETC

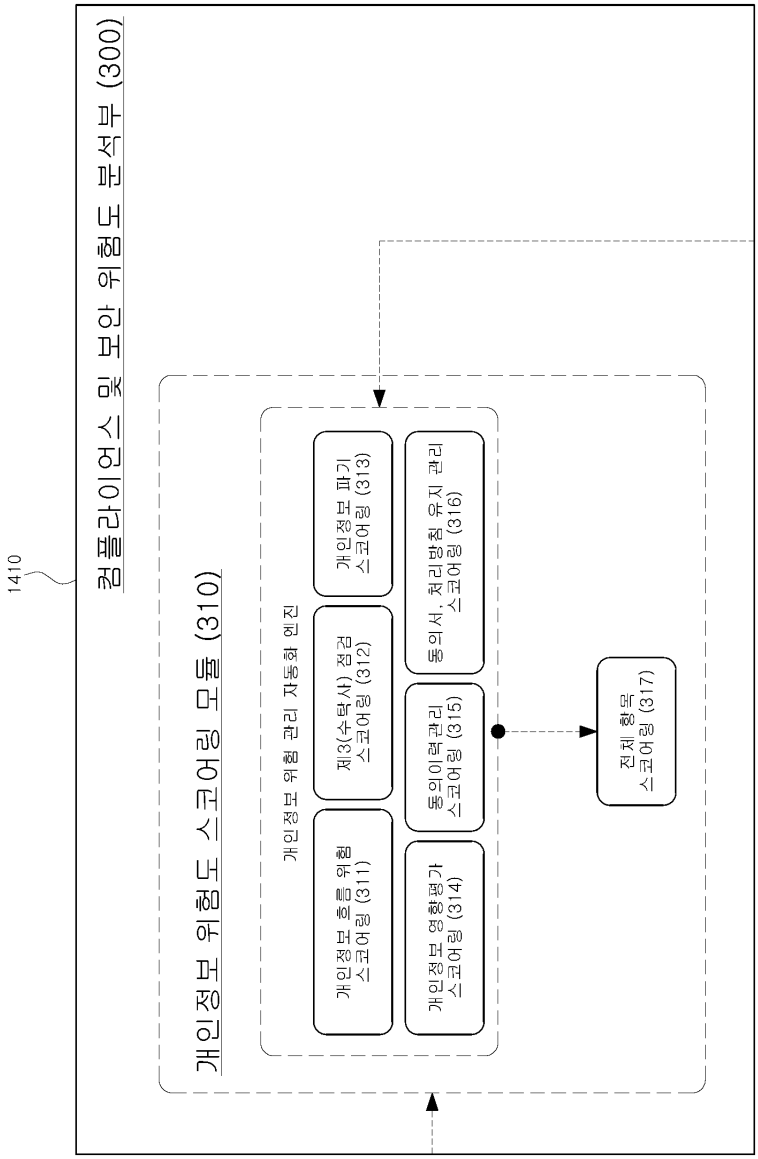
도면12


1210
개인정보처리방침 자동 생성 모듈
B4 모듈 (240)
서비스 분석 모듈 (241)
업종
규모
ETC
처리방침 구성 요소 생성 모듈 (242)
개인정보 수집 및 이용과 제공
가명정보 처리 여부
정보 보유 및 파기 정책
개인정보 위탁
3자 제공
국외 이전
보안 인력
처리방침 템플릿 반영 자동화 모듈 (243)
처리방침 템플릿

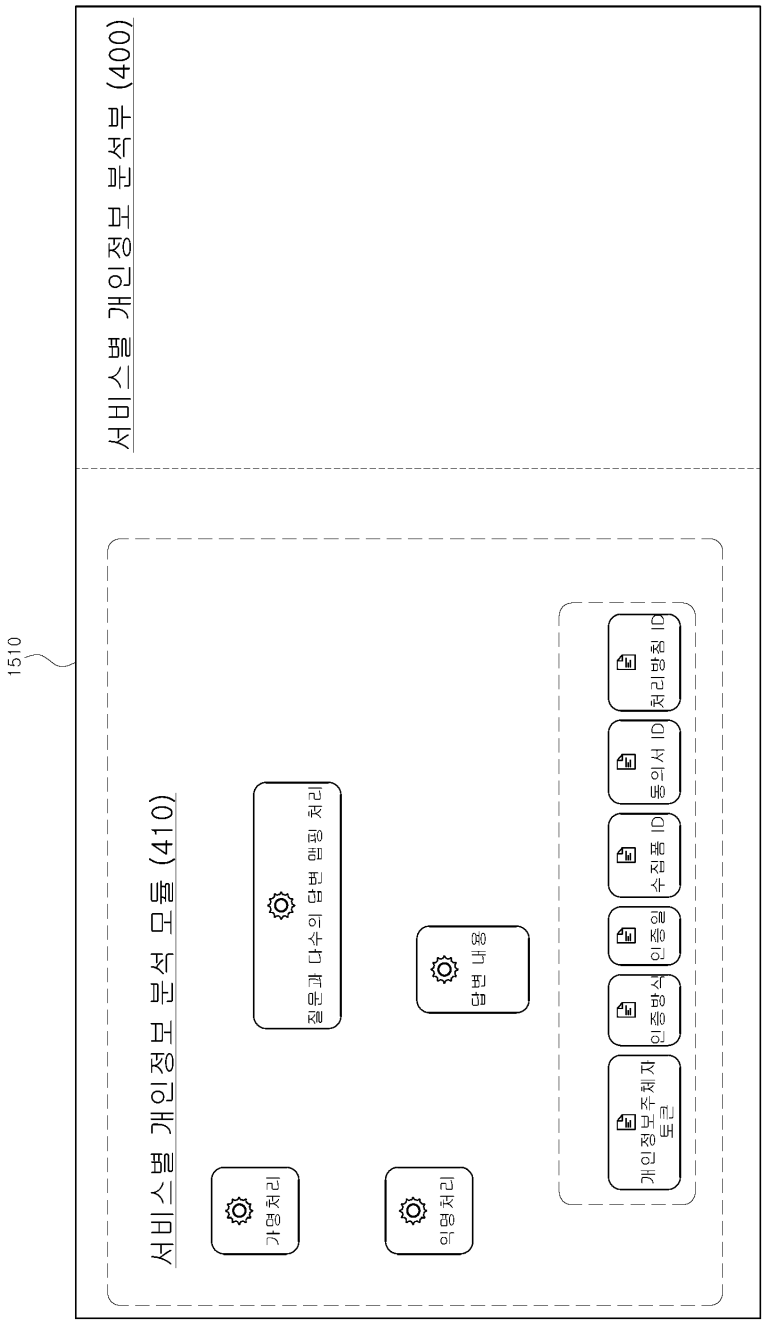
도면13


1310
개인정보주체자 토큰 및 동의이력 hash 생성 모듈 B5 모듈 (250)
제출정보
수집품 ID
개인정보
민감정보
고유식별번호
주민번호
3rd party (DID) (251)
휴대폰인증
본인인증
이메일인증
ETC
개인정보주체자 토큰
생성 모듈 (252)
주체자 유니크 값
인증방식
동의이력 Hash 생성 모듈 (253)
개인정보주체자 토큰
인증방식
인증일
수집품 ID
동의서 ID
처리방침 ID

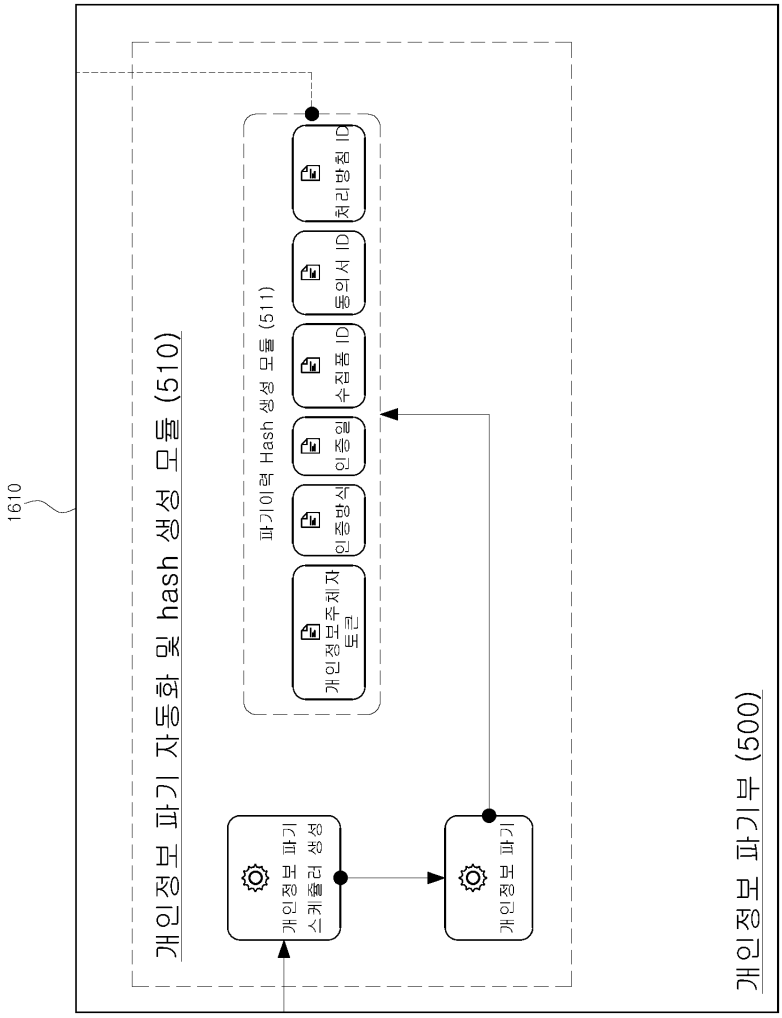
도면14


1410
컴플라이언스 및 보안 위험도 분석부 (300)
개인정보 위험도 스코어링 모듈 (310)
개인정보 위험 관리 자동화 엔진
개인정보 흐름 위험 스코어링 (311)
제3(수탁사) 점검 스코어링 (312)
개인정보 파기 스코어링 (313)
개인정보 영향평가 스코어링 (314)
동의이력관리 스코어링 (315)
동의서, 처리방침 유지 관리 스코어링 (316)
전체 항목 스코어링 (317)

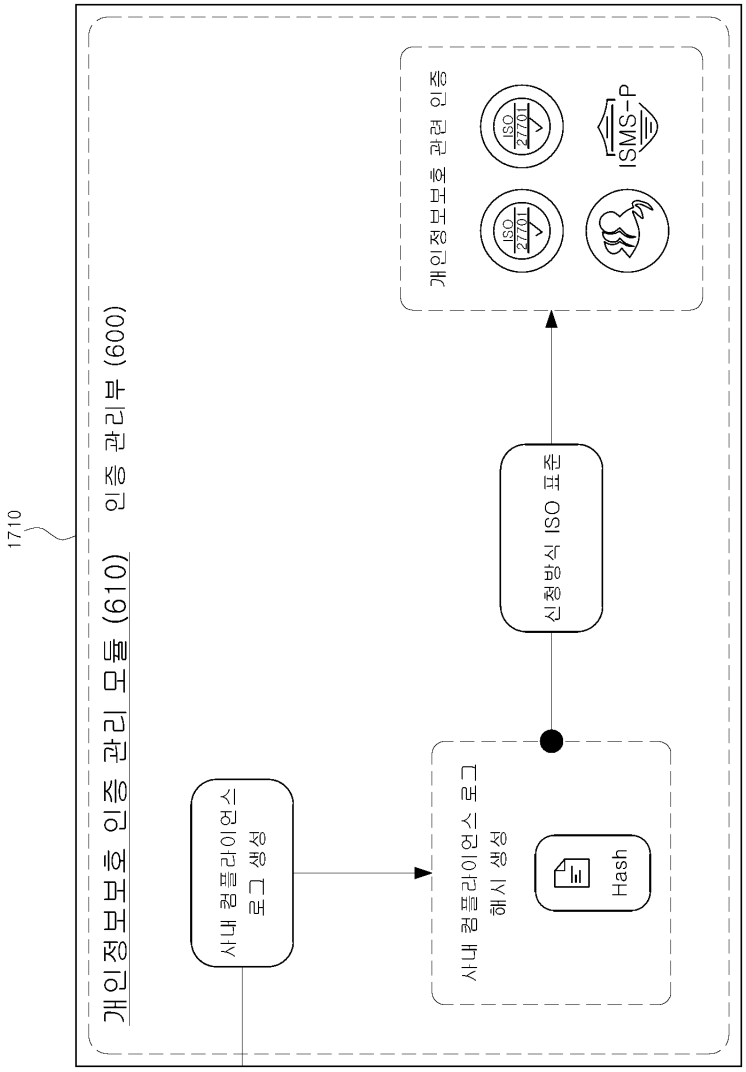
도면15


1510
서비스별 개인정보 분석부 (400)
서비스별 개인정보 분석 모듈 (410)
가명처리
질문과 다수의 답변 맵핑 처리
익명처리
답변 내용
개인정보주체자 토큰
인증방식
인증일
수집품 ID
동의서 ID
처리방침 ID

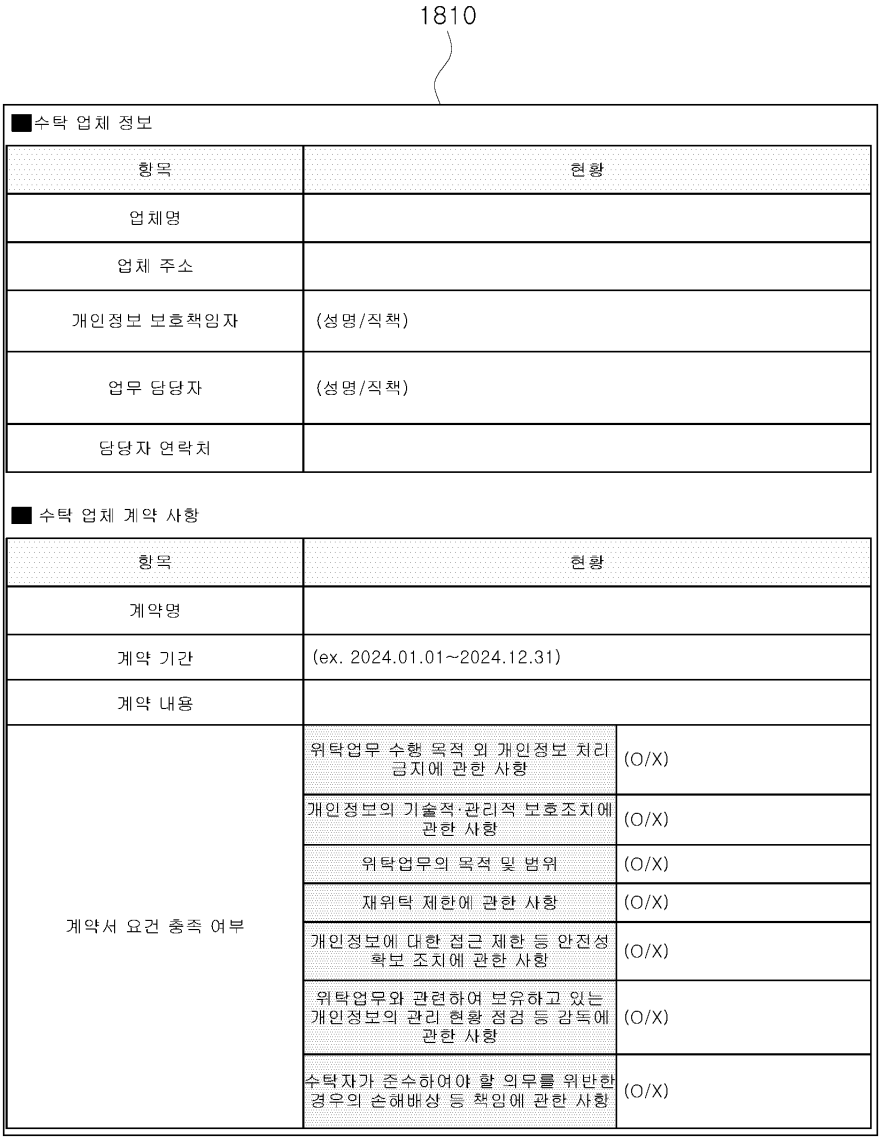
도면16


1610
개인정보 파기부 (500)
개인정보 파기 자동화 및 hash 생성 모듈 (510)
개인정보 파기 스케줄러 생성
개인정보 파기
파기이력 Hash 생성 모듈 (511)
개인정보주체자 또는
인증방식
인증일
수집품 ID
동의서 ID
처리방침 ID

도면17


1710
개인정보보호 인증 관리 모듈 (610)
인증 관리부 (600)
사내 컴플라이언스 로그 생성
사내 컴플라이언스 로그 해시 생성
Hash
신청방식 ISO 표준
개인정보보호 관련 인증
ISO 27701
ISO 27701
ISMS-P

도면18


1810
■수탁 업체 정보
항목
현황
업체명
업체 주소
개인정보 보호책임자
(성명/직책)
업무 담당자
(성명/직책)
담당자 연락처
■ 수탁 업체 계약 사항
항목
현황
계약명
계약 기간
(ex. 2024.01.01~2024.12.31)
계약 내용
계약서 요건 충족 여부
위탁업무 수행 목적 외 개인정보 처리 금지에 관한 사항
(O/X)
개인정보의 기술적·관리적 보호조치에 관한 사항
(O/X)
위탁업무의 목적 및 범위
(O/X)
재위탁 제한에 관한 사항
(O/X)
개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
(O/X)
위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
(O/X)
수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
(O/X)

도면19

1910

■ 개인정보 처리 현황

구분	항목		현황
개인정보 수탁업무 현황	수탁업무 목적		(ex. 처리 업무 대생, 이벤트 등)
	수탁업무 개인정보취급자 수		(ex. 100건)
	개인정보 취급항목		(ex. 이름, 이메일, 전화번호 등)
개인정보 제공	개인정보를 제공하는 위탁사 담당자		(ex. 보안팀/홍보호)
	제공받는 방법		(ex. 이메일, USB, 서명, 전용선, VPN 등)
개인정보 수집	자체 개인정보 수집 여부		(O/X)
	수집 현황	수집 방법	(ex. 서면, 홈페이지 가입 등)
		수집 목적	
		수집 항목	
		처리 기간	
개인정보 저장	저장 위치		(ex. 담당자 PC, 시스템 등)
	개인정보 암호화 여부		(ex. DRM, 오피스암호화 등)
개인정보 이용	개인정보처리시스템 명칭		(ex. AAA 시스템 등)
	개인정보처리시스템 접속 방법		(ex. ID, P/W, SMS 인증 등)
	개인정보 마스킹 여부		(ex. 전체 개인정보 마스킹, 전화번호 중간 4자리 마스킹 등)
	재위탁 여부		(O/X)
개인정보 파기	파기대상 및 주기	대상	
		주기	
	파기 방법		
	파기결과 보고 방법		

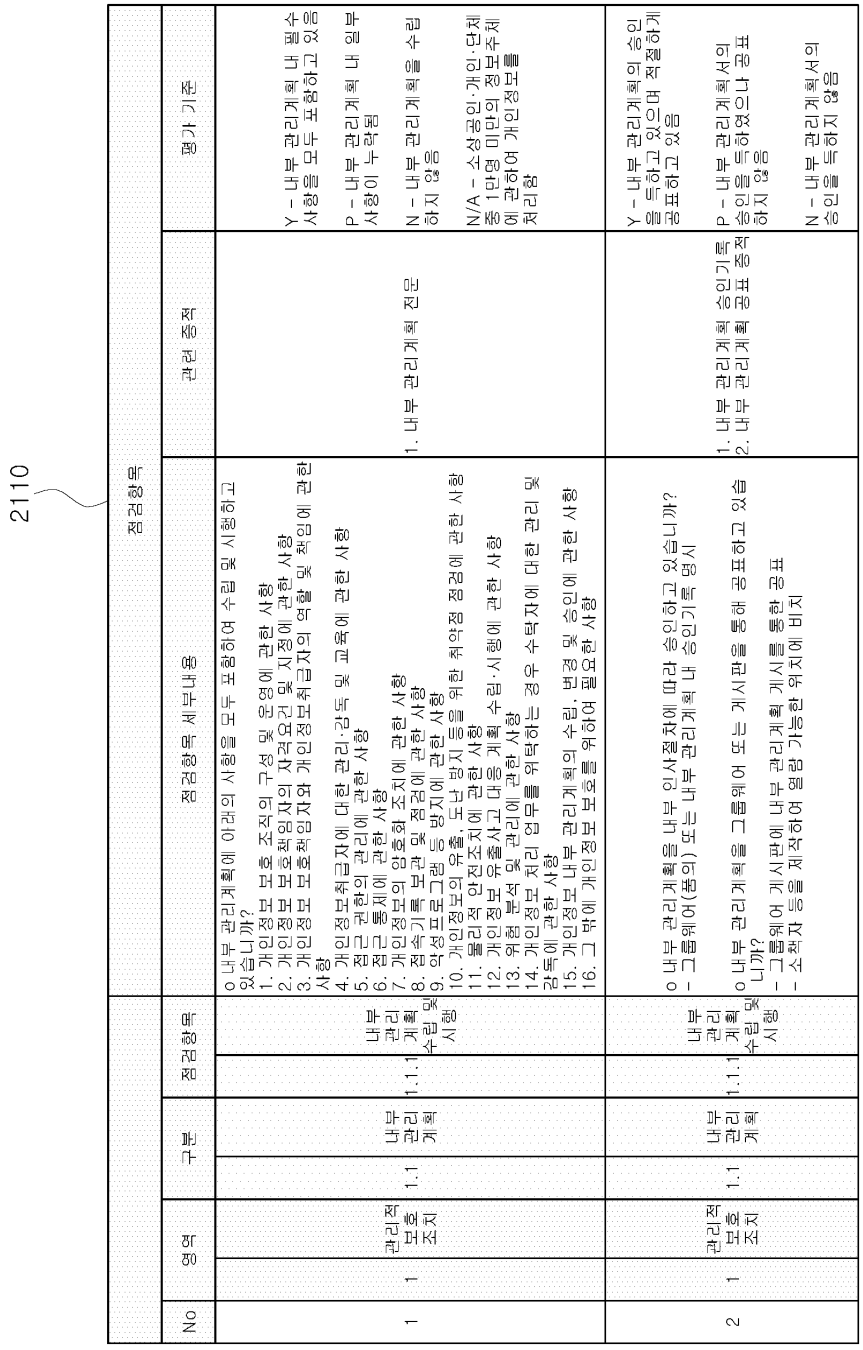
도면20

2010

■ 재위탁 업체 현황

항목	현황
상호	
재위탁 목적	
재위탁 개인정보 항목	(ex. 이름, 이메일, 전화번호 등)
재위탁된 개인정보 보유이용 기간	(ex. 이용목적 달성 즉시 등)
관리 및 감독 방법	
파기확인 방법	
위탁 계약서	

도면21


2110
점검항목
No
영역
구분
점검항목
점검항목 세부내용
관련 증적
평가 기준
1
관리적 보호 조치
내부 관리 계획 수립 및 시행
1.1
1.1.1
o 내부 관리계획에 아래의 사항을 모두 포함하여 수립 및 시행하고 있습니까?
1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 그 밖에 개인정보 보호를 위하여 필요한 사항
1. 내부 관리계획 전문
N - 내부 관리계획을 수립하지 않음
N/A - 소상공인·개인·단체 중 1단생 미만의 정보주체에 관하여 개인정보를 처리함
2
관리적 보호 조치
내부 관리 계획 수립 및 시행
1.1
1.1.1
o 내부 관리계획을 내부 인사절차에 따라 승인하고 있습니까?
- 그룹웨어(품의) 또는 내부 관리계획 내 승인기록 명시
o 내부 관리계획을 그룹웨어 또는 게시판을 통해 공표하고 있습니까?
- 그룹웨어 게시판에 내부 관리계획 게시를 통한 공표
- 소책자 등을 제작하여 열람 가능한 위치에 비치
1. 내부 관리계획 승인기록
2. 내부 관리계획 공표 증적
Y - 내부 관리계획의 승인을 득하고 있으며 적절하게 공표하고 있음
P - 내부 관리계획의 승인을 득하였으나 공표하지 않음
N - 내부 관리계획의 승인을 득하지 않음

도면22

2210

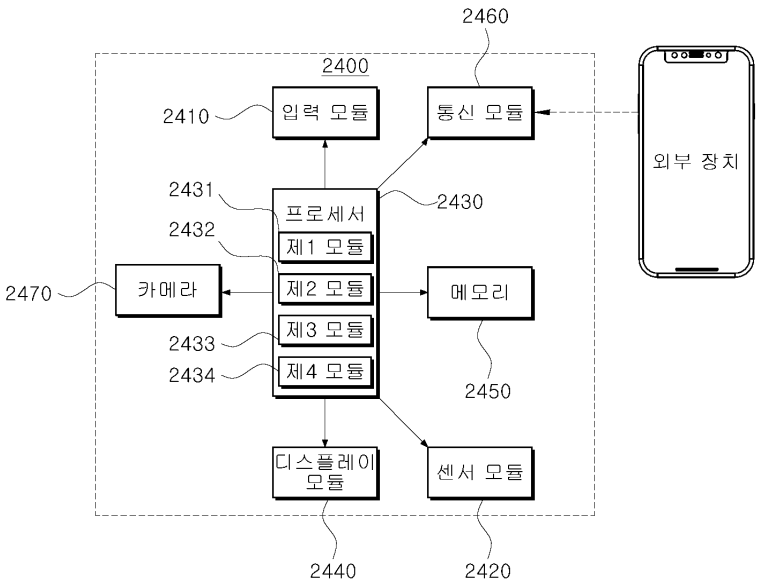
점검 현황		관련 법령	관련 고시
평가 결과 (Y, P, N, N/A)	운영 현황 (N/A일 경우 사유 작성)		
Y		o 개인정보 보호법 제29조 - 시행령 제30조	o 개인정보의 안전성 확보 조치 기준 제4조
		o 개인정보 보호법 제29조 - 시행령 제30조	o 개인정보의 안전성 확보 조치 기준 제4조

도면23

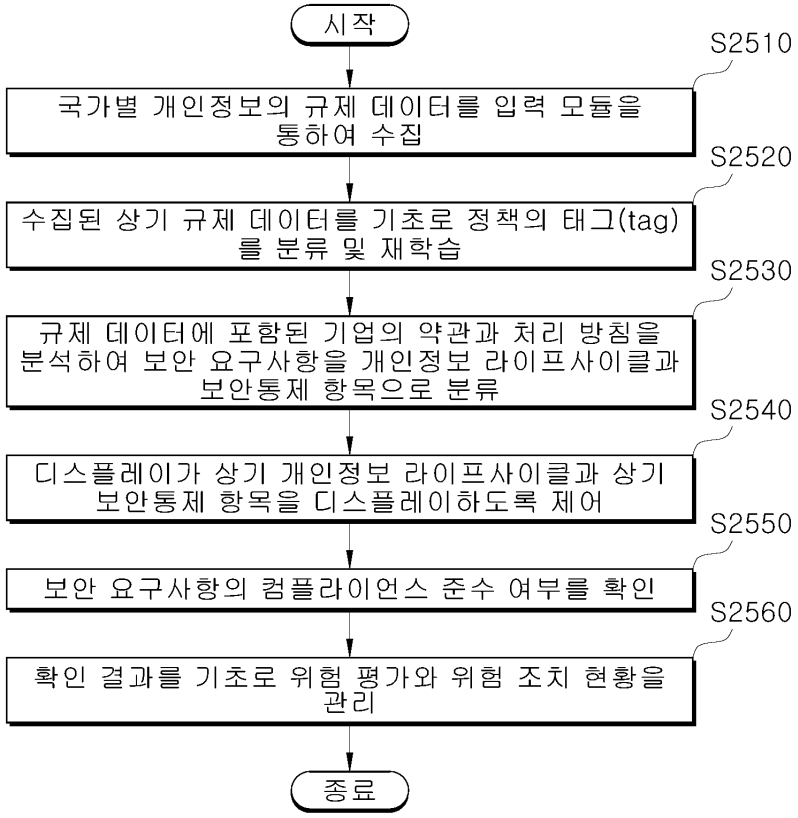
2310

벌칙				벌칙 규정
형벌		행정처분		
징역 (단위:이하)	벌금 (단위:이하)	과징금 (단위:이하)	과태료 (단위:이하)	
-	-	-	5천만원	o 개인정보 보호법 제75조 ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부가한다. 5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 운용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
-	-	-	5천만원	o 개인정보 보호법 제75조 ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부가한다. 5.3 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 운용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
-	-	-	5천만원	o 개인정보 보호법 제75조 ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부가한다. 5.3 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 운용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

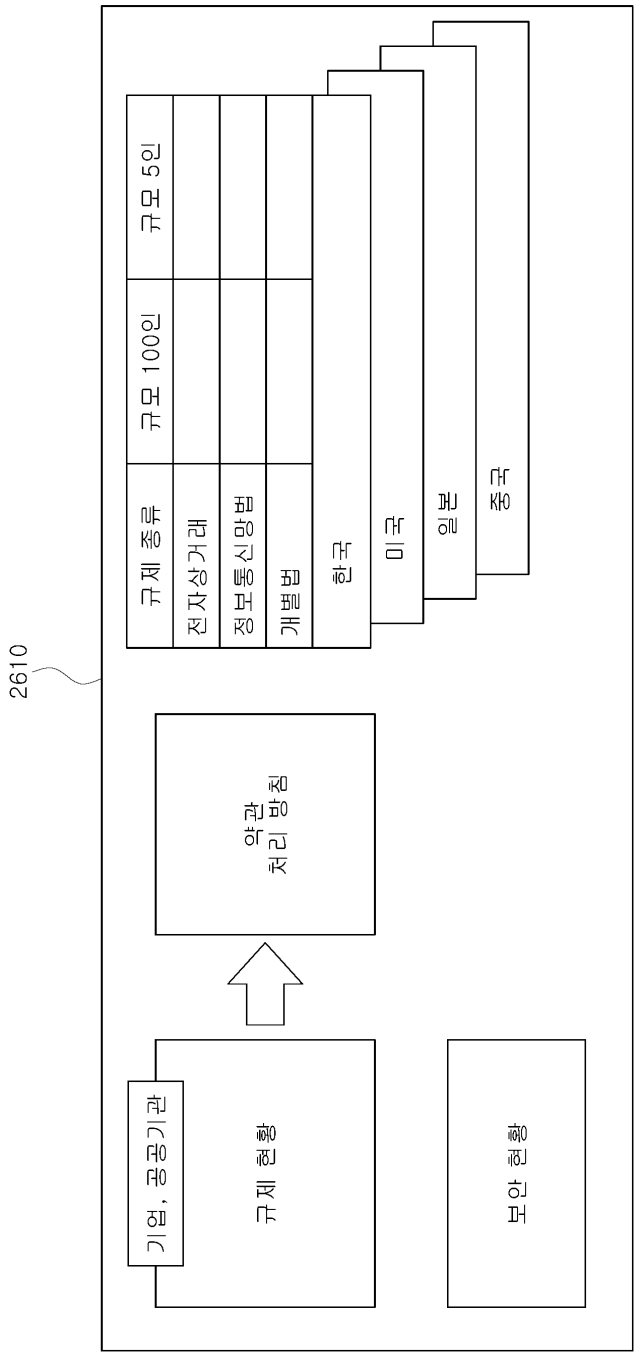
도면24



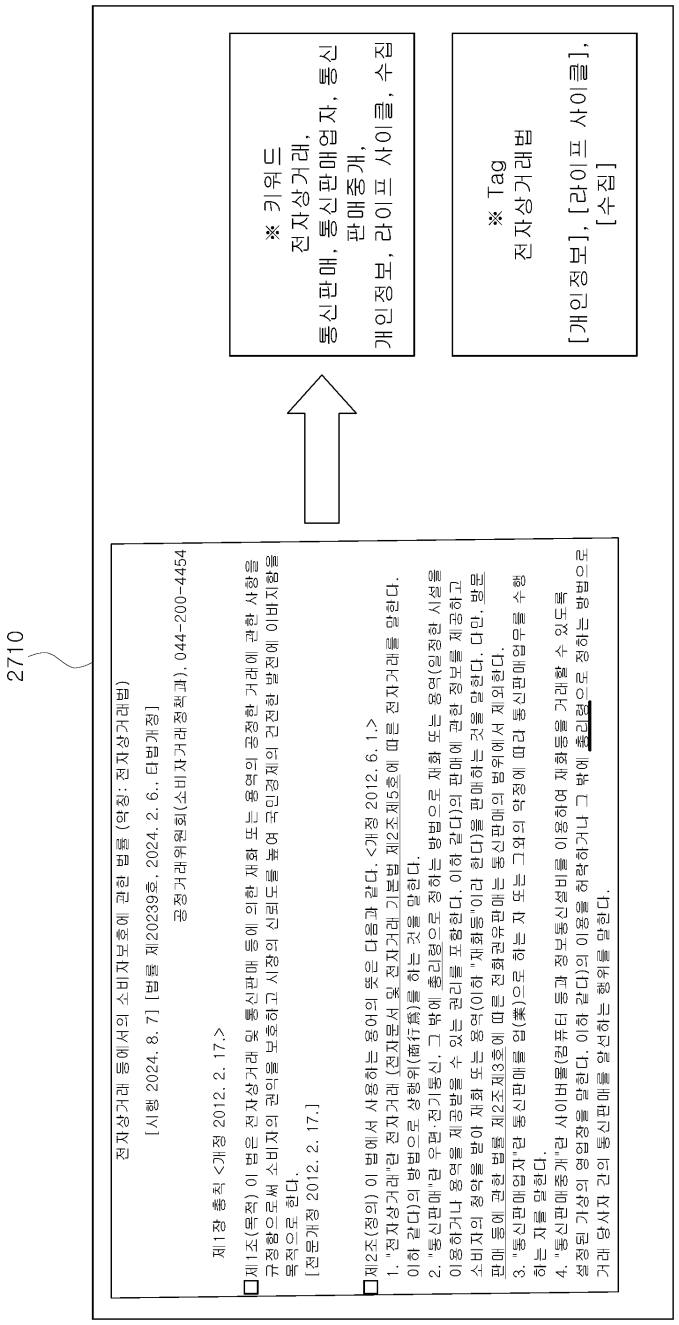
도면25


시작
S2510
국가별 개인정보의 규제 데이터를 입력 모듈을 통하여 수집
S2520
수집된 상기 규제 데이터를 기초로 정책의 태그(tag)를 분류 및 재학습
S2530
규제 데이터에 포함된 기업의 약관과 처리 방침을 분석하여 보안 요구사항을 개인정보 라이프사이클과 보안통제 항목으로 분류
S2540
디스플레이가 상기 개인정보 라이프사이클과 상기 보안통제 항목을 디스플레이하도록 제어
S2550
보안 요구사항의 컴플라이언스 준수 여부를 확인
S2560
확인 결과를 기초로 위험 평가와 위험 조치 현황을 관리
종료

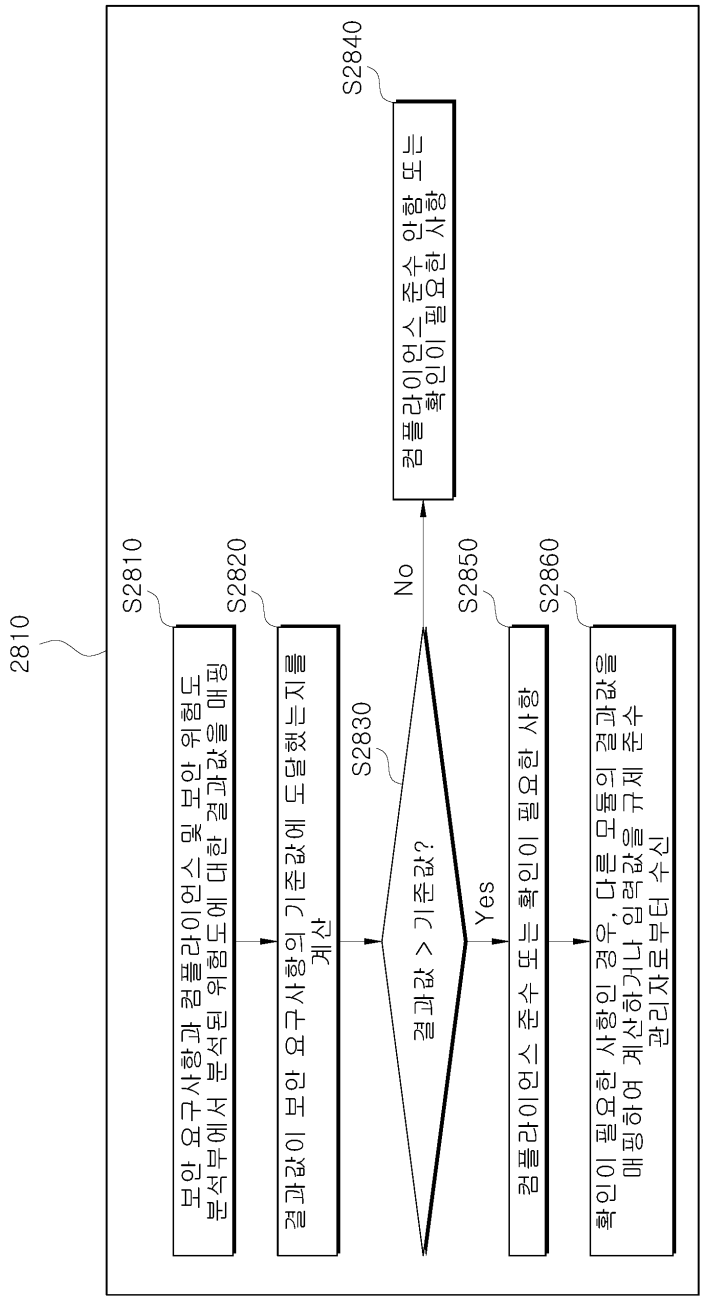
도면26


2610
기업, 공공기관
규제 현황
보안 현황
약관
처리 방침
규제 종류
규모 100인
규모 5인
전자상거래
정보통신망법
개별법
한국
미국
일본
중국

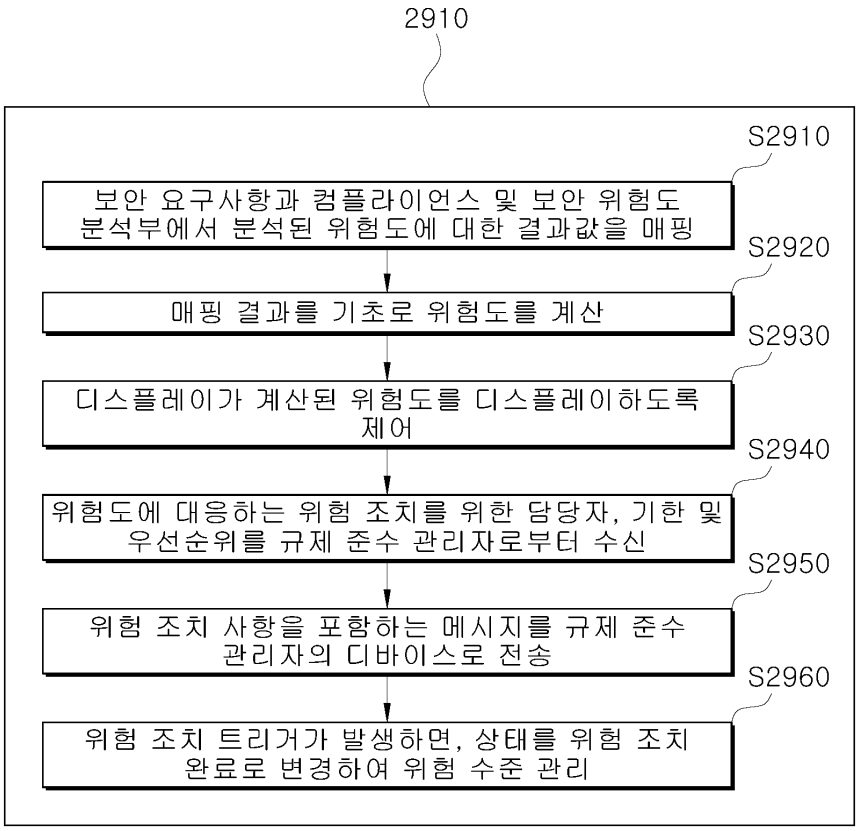
도면27


2710
전자상거래 등에서의 소비자보호에 관한 법률 (약칭: 전자상거래법)
[시행 2024. 8. 7] [법률 제20239호, 2024. 2. 6., 타법개정]
공정거래위원회(소비자거래정책과), 044-200-4454
제1장 총칙 <개정 2012. 2. 17.>
제1조(목적) 이 법은 전자상거래 및 통신판매 등에 의한 재화 또는 용역의 공정한 거래에 관한 사항을 규정함으로써 소비자의 권익을 보호하고 시장의 신뢰도를 높여 국민경제의 건전한 발전에 이바지함을 목적으로 한다.
[전문개정 2012. 2. 17.]
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2012. 6. 1.>
1. "전자상거래"란 전자거래 (전자문서 및 전자거래 기본법 제2조제5호에 따른 전자거래를 말한다. 이하 같다)의 방법으로 상행위(商行爲)를 하는 것을 말한다.
2. "통신판매"란 우편·전기통신, 그 밖에 총리령으로 정하는 방법으로 재화 또는 용역(일정한 시설을 이용하거나 용역을 제공받을 수 있는 권리를 포함한다. 이하 같다)의 판매에 관한 정보를 제공하고 소비자의 청약을 받아 재화 또는 용역(이하 "재화등"이라 한다)을 판매하는 것을 말한다. 다만, 방문판매 등에 관한 법률 제2조제3호에 따른 전화권유판매는 통신판매의 범위에서 제외한다.
3. "통신판매업자"란 통신판매를 업(業)으로 하는 자 또는 그 외의 약정에 따라 통신판매업무를 수행하는 자를 말한다.
4. "통신판매중개"란 사이버몰(컴퓨터 등과 정보통신설비를 이용하여 재화등을 거래할 수 있도록 설정된 가상의 영업장을 말한다. 이하 같다)의 이용을 허락하거나 그 밖에 총리령으로 정하는 방법으로 거래 당사자 간의 통신판매를 알선하는 행위를 말한다.
※ 키워드
전자상거래,
통신판매, 통신판매업자, 통신
판매중개,
개인정보, 라이프 사이클, 수집
※ Tag
전자상거래법
[개인정보], [라이프 사이클],
[수집]

도면28


2810
S2810
보안 요구사항과 컴플라이언스 및 보안 위험도 분석부에서 분석된 위험도에 대한 결과값을 매핑
S2820
결과값이 보안 요구사항의 기준값에 도달했는지를 계산
S2830
결과값 > 기준값?
No
S2840
컴플라이언스 준수 안함 또는 확인이필요함 사항
Yes
S2850
컴플라이언스 준수 또는 확인이 필요한 사항
S2860
확인이 필요한 사항인 경우, 다른 모듈의 결과값을 매핑하여 계산하거나 입력값을 규제 준수 관리자로부터 수신

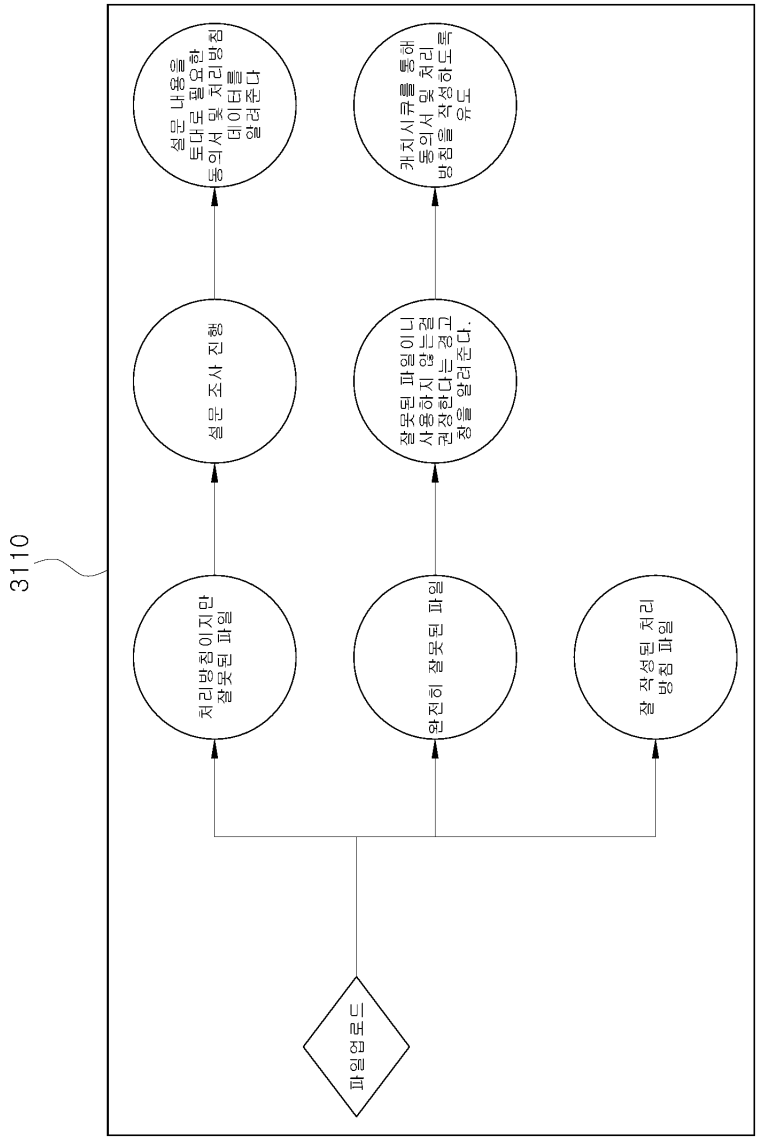
도면29


2910
S2910
보안 요구사항과 컴플라이언스 및 보안 위험도 분석부에서 분석된 위험도에 대한 결과값을 매핑
S2920
매핑 결과를 기초로 위험도를 계산
S2930
디스플레이가 계산된 위험도를 디스플레이하도록 제어
S2940
위험도에 대응하는 위험 조치를 위한 담당자, 기한 및 우선순위를 규제 준수 관리자로부터 수신
S2950
위험 조치 사항을 포함하는 메시지를 규제 준수 관리자의 디바이스로 전송
S2960
위험 조치 트리거가 발생하면, 상태를 위험 조치 완료로 변경하여 위험 수준 관리

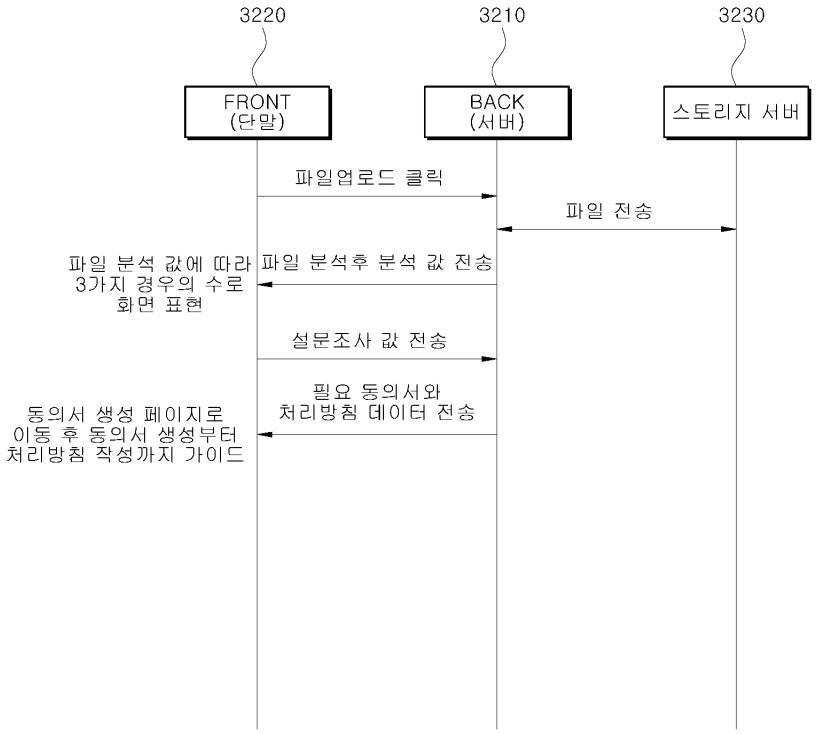
도면30


3010
개인정보 처리방침
수정하기
4cf9194f-7a9e-413... 7 / 10
46%
4
5
개인정보 처리항목
처리방침 시행일
2024-08-27

도면31


3110
파일업로드
처리방침이지만
잘못된 파일
원진히 잘못된 파일
잘 작성된 처리
방침 파일
설 문 조사 진행
잘못된 파일이니
사용하지 않는걸
권장한다는 경고
창을 알려준다.
캐치시큐를 통해
동의서 및 처리
방침을 작성하도록
유도
설문 내용을
토대로 필요한
동의서 및 처리방침
데이터를
알려준다

도면32


3220
3210
3230
FRONT
(단말)
BACK
(서버)
스토리지 서버
파일업로드 클릭
파일 전송
파일 분석 값에 따라
3가지 경우의 수로
화면 표현
파일 분석후 분석 값 전송
설문조사 값 전송
필요 동의서와
처리방침 데이터 전송
동의서 생성 페이지로
이동 후 동의서 생성부터
처리방침 작성까지 가이드