정보보호정책

조직의 내/외부 환경과 업무 성격에 맞는 효과적인 정보보호를 위하여 기본적으로 무엇이 수행되어야 하는가를 일목요연하게 기술한 지침과 규약
조직의 정보보호 목적과 활동에 고나한 사항을 정의한 최상위 문서

(포함되어야할 내용)

- 조직의 정보보호에 대한 최고경영자 등 경영진의 의지 및 방향
- 조직의 정보보호에 대한 역할과 책임 및 대상과 범위
- 조직이 수행하는 관리저/기술적/물리적 정보보호 활동의 근거

(승표 과정)

1) 이해관계자와 정책 내용을 충분히 협의/검토한다
2) 최고경영자 또는 최고경영자로부터 권한을 위임받은 자의 승인을 받아야 한다
3) 최신본을 임직원과 관련자에게 이해하기 쉬운 형태로 전달

정보보호정책을 구현하기 위한 요소

1) 표준(Standards)

- 정보보호정책의 달성을 위해 필요한 세부 요구사항을 구체적으로 정의한 규정으로 관련된 모든 사용자가 준수하도록 요구되는 강제성을 가지는 사항들을 설명한 문서

2) 지침(Guidelines)

- 정보보호정책에 따라 특정 시스템 또는 특정 분야별로 활동이 필요하거나 도움이 되는 세부 요구사항에 관한 규정으로 강제성보다는 권고적이고 융통성 있게 적용할 수 있는 사항들을 설명한 문서

3) 절차(Procudure)

- 정책/표준/지침을 준수하기 위하여 구체적으로 어떻게 해야하는지를 세부적으로 상세하게 설명한 문서
- 수행해야 할 업무들을 순서에 따라 단계적으로 설명
- 정보보호 활동의 구체적 적용을 위해 필요한 적용 절차 등의 구체적이고 세부적인 방법을 기술

위험의 구성 요소

자산

위협

취약점

+1 보호대책(정보보호대책)

위험 관리

보호 대책을 마련하는 일련의 과정

위험 관리를 위한 구성요소 +1

위험 : 자산의 취약성을 이용한 위협에 의해 원하지 않는 사건이 발생하여 자산에 손실을 미칠 가능성

위협 : 자산에 손실을 초래할 수 있는 원하지 않는 사건의 잠재적 원인 또는 행위자

취약점 : 위협의 이용 대상이 되는 자산의 잠재적 속성(기술적, 관리적, 물리적 약점)

위험 관리 과정

1) 위험관리 전략 및 계획 수립 : 조직에 적합한 위험관리(분석) 방법론을 선택하고 비용과 시간, 인력 등 가용자원을 고려하여 계획을 수립하는 단계

2) 위험 분석 : 위험을 분석하고 해석하는 과정으로 조직의 자산에 취약점을 식별하고 식별한 정보자산의 가치를 평가하기 위한 과정이 필요하며, 위협을 분석하여 위험의 내용과 정도를 결정하는 과정

3) 위험 평가 : 위험 분석 결과를 기초로 위험도를 평가하고 조직에서 수용가능한 목표 위험 수준(DoA)을 정하여 이를 기준으로 위험의 대용 여부와 우선 순위를 결정하

4) 정보보호대책 선정 : 위험 평가에 기초하여 위험 대응에 필요한 보호 대책을 선정하는 단계

5) 정보보호 계획 수립 : 선정한 보호 대책을 구현할 계획(이행 계획)을 수립하는 단계

위험 분석 접근 방법

1) 기준선(베이스라인) 접근법
- 모든 자산에 대한 체크리스트 형식의 표준화된 보호 대책을 이용하여 보호의 기본 수준을 정하고 위험분석을 수행하는 접근법
(장단점) : 시간과 비용이 많이 들지 않고 모든 조직에서 기본적으로 필요한 보호 대책 선택이 가능하지만, 조직의 특성을 고려하지 않기 때문에 과보호 또는 부족한

2) 비정형 접근법
- 정형화된 위험 분석 방법론을 사용하지 않고 경험자의 지식을 기반으로 위험 분석을 수행하는 접근법
(장단점) 작은 규모의 조직에 비용 대비 효과적이지만 수행자의 경험이 부족한 위험 영역을 놓칠 가능성이 있다

3) 상세 위험 분석
- 정형화되고 구조화된 위험 분석 방법론에 따라 자산 분석, 위협 분석, 취약섬 분석등의 각 단계를 통해 조직의 중요한 위험들을 모두 상세하게 분석하는 접근법
(장단점) 조직에 가장 적절한 보호 대책을 수립할 수 있지만 결과를 얻기 위해 전문적인 지식, 많은 시간과 노력이 요구됨

4) 복합 접근법(Combined approach)
- 고위험 영역을 식별하여 상세 위험 분석을 수행하고 그 외의 영역은 기준선 접근법을 사용하는 접근법
(장단점) 위험 분석 비용과 자원을 효과적으로 사용할 수 있으며 고위험 영역을 빠르게 식별하고 적절하게 처리할 수 있지만, 고위험 영역이 잘못 식별 되었을 경우 비

위험 분석(상세 위험 분석) 절차

1) 자산 분석(자산 식별 및 자산 가치 평가) : 보호해야 할 자산을 식별하고 자산별 기밀성, 무결성, 가용성 측면의 중요도에 따라 가치를 평가

2) 위협 평가 : 자산에 대한 위협을 식별하고 위협이 자산에 미치는 영향(위협의 발생 가능성, 영향 정도)을 평가한다

3) 취약성(취약점) 분석 : 식별된 위협에 대한 자산의 취약성을 식별하고 자산에 미치는 영향을 평가한다

다)

5) 위험 평가 : 자산 분석, 위협 및 취약성 평가, 기존 보호대책 평가 결과를 이용하여 최종적으로 자산의 위험도(위험 수준, 잠재적 손실의 규모)를 평가한다

상세 위험 분석 절차 중 자산 분석 단계의 내용

담고 있어야 하며 중복이나 누락된 자산이 없어야 한다

(자산 가치 평가) 자산이 식별되면 자산별 기밀성, 무결성, 가용성 측면에서 중요도를 산정하고 중요도에 따라 자산의 가치를 평가한다

업을 반복하지 않음으로써 시간과 비용을 최소화 할 수 있다

정성적 위험 분석 방법론
델파이법 : 각 분야의 전문적인 지식을 갖춘 전문가 집단을 구성하고 토론을 통해 위험분석 및 평가를 수행하는 방법
시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대한 발생 가능한 결과들을 추정하는 방법
법
퍼지행렬법 : 자산, 위험, 보안체계등 위험 분석 요소들을 정성적인 언어로 표현된 값을 사용하여 기대 손실을 평가하는 방법
업무 연속성 계획(BCP : Business Continuity Plan)
차)
업무 연속성 계획의 5단계
1) 프로젝트 범위 설정 및 기획 : 프로젝트 계획 수립(범위, 조직, 기간, 인원 등을 정의)
2) 사업영향평가(BIA) : 개별 업무 중단 시 손실 영향도 파악(복구 우선순위, 복구 목표 시간 및 수준)
3) 복구전략개발 : 복구 자원 및 복구 방안들에 대한 평가
4) 복구계획수립 : 실제 복구 계획 수립 및 명시적 문서화
5) 프로젝트 수행 테스트 및 유지 보수 : 테스트 및 유지보수 관리 절차 수립
업무 영향 분석(BIA: Business Impact Analysis)
결정하는 과정
1) 핵심(주요) 업무 프로세스의 식별
2) 재해 유형 식별 및 재해 발생 가능성과 발생 시 업무중간의 지속시간 평가
3) 업무 프로세스별 중요도 및 재해로 인한 업무중단 시의 손실 평가
4) 업무 프로세스별 우선순위 및 복구 대상 범위의 설정
5) 재해 발생 시의 업무 프로세스의 복원 시간이나 우선순위 결정
재해 복구 관련 용어
재해 복구(DR) : 재해로 인하여 중단된 정보기술(IT) 서비스를 재개하는 것
재해복구계획(DRP) : 정보기술 서비스 기반에 대하여 재해가 발생할 경우 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획
재해복구시스템(DRS) : 재해복구계획의 원활한 수행을 지우너하기 위하여 평상시에 확보하여 두는 인적/물적 자원 및 이들에 대한 지속적인 관리체계가 통합된 것
복구 목표 시간(RTO) : 재해로 인해 서비스가 중단되었을 때, 서비스를 복구하는데까지 걸리는 최대 허용 시간
복구 목표 시점(PRO) : 재해로 인하여 중단된 서비스를 복구하였을 때, 유실을 감내할 수 있는 데이터의 손실 허용 시점
ISMS-P 관련 용어
기관이 증명하는 것을 말한다

정보보호 관리체계 인증 : 인증 신청인의 정보보호 관현 일련의 조치와 활동이 인증기준에 적합함을 인터넷 진흥원 또는 인증기관이 증명하는 것을 말함
인증기관 : 인증에 관한 업무를 수행할 수 있도록 과학기술정보통신부장관과 개인정보 보호위원회가 지정하는 기관을 말한다
심사기관 : 인증심사 업무를 수행할 수 있도록 과학기술정보통신부장관과 개인정보보호위원회가 지정하는 기관을 말한다
최초 심사 : 처음으로 인증을 신청하거난 인증범위에 중요한 변경이 있어서 다시 인증을 신청했을 때 실시하는 인증심사를 말한다
사후 심사 : 인증받고 난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다
갱신 심사 : 유효기간 만료로 유효기간 갱신을 위해 실시하는 인증심사를 말한다,
ISMP-P인증기준 - 보안대책 요구사항 - 물리적 정보보호
보호구역 지정 : 통제구역/제한구역/접견구역 등 물리적 보호구역을 지정하고 구역별 보호대책을 수립 이행
출입 통제 : 보호구역은 인가된 사람만이 출입하도록 통제하고 출입 이력을 주기적으로 검토해야 한다.
정보시스템 보호 : 정보시스템의 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호해야 한다
보호설비 운영 : 정보시스템의 중요도와 특성을 고려하여 적절한 보호설비를 갖추고 운영해야 한다
보호구역 내 작업 : 보호구역 내 작업 절차를 수립/이행하고 작업 기록을 주기적으로 검토
반출입 기기 통제 : 보호구역 내 장비 반출입 통제절차를 수립/이행하고 작업 기록을 주기적으로 검토
업무환경 보안 : 업무환경에서 개인정보 및 중요정보가 노출되지 않도록 클린데스크, 정기 점검 등 보호 대책을 수립/이행
개인정보 보호법 및 개인정보의 안전성 확보조치 기준
정보주체 : 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
개인정보처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인등
개인정보 보호책임자 : 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자
개인정보취급자 : 개인정보 처리자의 지휘/감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등
이용자 : 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자
개인정보파일 : 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물
개인정보처리시스템 : 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템
말한다.
위험도 분석 : 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별/평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적 분석행위
을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보
생체인식정보 : 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보
가진 자라는 것을 식별할 수 있도록 시스템에 전달해야하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
내부망 : 인터넷망 차단, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간

수행업무 등을 전자적으로 기록한 것

내부 관리계획 : 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립/시행하는 내부 기준

개인정보처리자의 개인정보 안전성 확보 조치의 기준에 따른 분류

[관리적 조치]
- 개인정보의 안전한 처리를 위한 내부 관리계획의 수립/수행 및 점검

[기술적 조치]
- 개인정보에 대한 접근 권한을 제한하기 위한 조치
- 개인정보에 대한 접근을 통제하기 위한 조치
- 개인정보를 안전하게 저장/전송하는데 필요한 조치
- 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조/ 변조 방지를 위한 조치
- 개인정보처리시스템 및 개인 정보 처리에 이용하는 정보기기에 대해 컴퓨터 바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검/치료할 수

[물리적 조치]
- 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치등 물리적 조치

개인정보의 안전성 확보조치 기준의 접속기록의 보관 및 점검 관련 사항

개인정보처리자는 개인정보 취급자의 개인정보처리시스템에 대한 접속기록은 1년이상 보관/관리 해야함
단, 2년이상 해야하는 경우
- 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
- 고유식별정보 또는 민감정보을 처리하는 개인정보처리시스템에 해당하는 경우

개인정보처리자는 개인정보의 오남용, 분실/도난/유출/위조/변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록등을 월 1회이상 점검해야한다
특히, 개인정보의 다운로드가 확인된 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다

개인정보 이용/제공 내역의 통지

1) 통지의무 대상 개인정보처리자
- 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자
- 100만명 이상의 정보주체에 대한 개인정보를 처리하는 자

2) 통지해야하는 정보
- 개인정보의 수집/이용 목적 및 수집한 개인정보 항목
- 대인정보를 제공받은 제3자와 그 제공 목적 및 제공한 개인정보 항목

3) 통지 방법 및 주기
- 연 1회이상
- 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법
- 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법

개인정보의 안전성확보조치 기준의 재해/재난 대비 안전조치

1) 조치 해야할 대상 - 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업/중견기업/공공기관에 해당하는 개인정보처리자 - 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업/단체에 해당하는 개인정보처리자
2) 조치사항 - 위기대응 매뉴얼 등 대응절차를 말녀하고 정기적으로 점검 - 개인정보처리시스템 백업 및 복구를 위한 계획을 마련
개인정보의 수집/이용에 따른 정보주체 동의 시 고지사항
1) 개인정보의 수집/이용 목적
2) 수집하려는 개인정보 항목
3) 개인정보의 보유및 이용 기간
4) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
개인정보의 제3자 제공에 따른 정보주체 동의 시 고지사항
1) 개인정보를 제공받는 자
2) 개인정보를 제공받는 자의 개인정보 이용목적
3) 제공하는 개인정보의 항목
4) 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
업무용 모바일 기기 보호조치
비밀번호, 패턴, PIN, 지문 홍채 등을 사용하여 화면잠금 설정
디바이스 암호화 기능을 사용하여 애플리케이션, 데이터 등 암호화
UISM 카드에 저장된 개인정보 보호를 위한 USIM카드 잠금 설정
모바일 기기의 도난 또는 분실 시 원격 잠금, 데이터 삭제 등을 위해 제조사별로 지원하는 '킬스위치'나 이동통신사의 '잠금 웹 서비스'를 이용 *킬 스위치 : 분실한 스마트폰 등의 모바일 기기 내의 정보를 원격으로 삭제하거나 기기를 사용할 수 없도록 하는 모바일 기기 제조사에서 제공하는 서비스
중요한 개인정보를 처리하는 모바일 기기는 MDM 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등을 수행 *MDM : Moblie Device Management, 무선망을 이용해서 원격으로 스마트폰 등의 모바일 기긱를 제어하는 솔루션으로 분실된 모바일 기기의 위치 추적, 잠금 설정,
정보보호 최고책임자
대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 책임자로 지정하고 과학기술정보통신부장관에게 신고

(업무)
- 정보보호 계획의 수립/시행 및 개선
- 정보보호 실태와 관행의 정기적인 감사 및 개선
- 정보보호 위험의 식별 평가 및 정보보호 대책 마련
- 정봅보호 교육과 몸의 훈련 계획의 수립 및 시행

윈도우 운영체제의 정보를 수집하기 위한 시스템 내장 명령어

시스템 날짜와 시간 정보 : date /t & time /t

시스템의 호스트 이름 정보 : hostname 명령

시스템에 현재 접속한 사용자 정보 : whoami 명령

망분리(인터넷 망 차단 조치)

한다

1) 인터넷 망 가상화 방식
- 가상화된 인터넷 환경 제공으로 인한 악성 코드 감염을 최소화할 수 있다
- 인터넷 환경이 악성코드에 감염되거나 해킹을 당해도 업무 환경은 안전하게 유지할 수 있다

2) 업무망 가상화 방식
- 가상화 서버 환경에 업무정보가 저장됨에 따라 업무 데이터에 중앙 관리 및 백업이 용이하고 내부정보 유출 방지 효과가 증가한다
- 사용자 통제 및 관리 정책의 일괄적용이 가능하다

클라우드 서비스 유형

IaaS : 이용자에게 서버, 스토리지, 네트워크 등 하드웨어 인프라 자원만을 제공하는 서비스
(ISMS 인증 신청기관이 클라우드 서비스를 이용할 경우 대상 서비스 및 자산) : 신청기관이 직접 관리하는 서버OS, DB, 미들웨어, 응용프로그램

PaaS : 이용자에게 애플리케이션을 개발, 테스트, 배포하는 데 필요한 운영체제, 개발환경 플랫폼, 개발 언어 프레임워크 등을 제공하는 서비스
(ISMS 인증 신청기관이 클라우드 서비스를 이용할 경우 대상 서비스 및 자산) : 신청기관이 직접 관리하는 응용프로그램. 단, 클라우드 서비스 제공자로부터 계

SaaS : 이용자에게 클라우드 환경에서 동작하는 애플리케이션을 제공하는 서비스
(ISMS 인증 신청기관이 클라우드 서비스를 이용할 경우 대상 서비스 및 자산) : 응용프로그램 관련하여 신청기관이 관리 가능한 영역에 한해 심사 수행

DaaS : 가상 데스크톱 기술을 활용하여 사용자에게 가상 데스크톱환경을 제공하는 서비스

정보자산 그룹핑

정보자산 분석 시 유형, 중요도, 사용 용도, 위험 등이 유사한 자산들을 하나의 그룹으로 만들어 분류하는 것

(장점) 유형, 중요도 등이 유사한 정보자산을 그룹핑하여 동일한 위험분석 및 평가 작업을 반복하지 않음으로써 시간과 비용을 최소화할 수 있다.

기업업무관점에서 BYOD정책

개인 모바일 기기를 업무에 활용하는 정책 / 시간과 공간의 제약 없이 쉽게 업무 지원을 가능하게 하여 업무의 효율성과 편의성 제공

(대분류에 대한 분석 또는 개요)

1) MDM(Moblie Device Management)

- 기업 업무환경에서 모바일 기기를 원격으로 보호하고 감시하는 솔루션으로 애플리케이션 배포, 데이터 및 환경설정, 기기 잠금, 데이터 삭제 등 다양한 보안 기능을 제공

2) 모바일 가상화(Hypervisors)

- 하나의 모바일 기기에 가상화 기술을 이용하여 개인용과 업무용 운영체제를 동시에 설치하는 솔루션으로 평상시 개인용 운영체제로 모바일 기기를 사용하다가 업무를 해야 할 때 업무용 운영체제로 전환하여 사용한다

정보공유/분석 센터

전자적 침해행위에 대한 정보분석과 침해사고의 효율적 대응을 위한 관리체계

(역할)

- 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
- 침해사고가 발생하는 경우 실시간 경보/분석체계 운영

개인정보 영향평가

는 영향을 사전에 조사/예측/검토하여 개선 방안을 도출하고 이행 여부를 점검하는 체계적인 절차

이 목적

<위험도 산정>

위험도 = 개인정보 영향도 + (침해요인 발생가능성 X 법적 준거성) X 2

- 개인정보 처리업무 내 개인정보의 조합수준, 등급 등에 따라 개인정보 처리업무의 중요도(개인정보 영향도)를 산정
- 개인정보 처리업무의 중요도, 침해요인 발생가능성, 법률에 규정된 의무사항(법적 준거성) 등을 종합적으로 고려하여 도출한 위험도 산정방법

개인정보 영향평가의 대상의 기준

- 구축/운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
- 구축/운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축/운용하고 있는 다른 개인정보파일과 연계하여는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
- 구축/운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

CC(정보시스템 공통평가기준)의 주요 요소

*정보시스템(it 제품)의 보안성을 평가하기 위한 ISO/IEC 국제 표준

1) 평가 대상(TOE)

- 정보시스템의 보안성 평가범위를 정의한 것
- 신청기관은 정보시스템의 보안 기능성 일부 또는 전체를 평가범위로 정할 수 있다

2) 보호 프로파일(PP)

- 평가대상 유형별 보안 기능 요구사항을 기술한 문서
- 특정 제품 구현과 독립적으로 정의
- 일반적으로 관련된 사용자 그룹에 의해 특정 목적으로 생성됨

3) 보안 목표 명세서(ST)
- 평가대상의 세부 보안 기능 요구사항과 구현 내용을 기술한 문서로 평가의 근거로 사용
- 특정 제품 구현에 종속적으로 정의

4) 평가보증등급(EAL)
- 평가대상의 보증 수준을 판단하는 척도를 정의한 등급으로 해당 등급을 구성하는 보증 컴포넌트 패키지로 이루어져 있다
- EAL1(최저 등급)부터 EAL7(최고 등급)까지 7개 등급으로 구분되며 등급이 높아질수록 보증 수준이 높아짐을 의미
- 등급이 높아질수록 평가 노력도(범위, 상세, 엄격)가 증가하여 평가 기간과 비용이 늘어난다.

개인정보 수집이 가능한 경우

1) 정보주체의 동의를 받은 경우

2) 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

3) 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

4) 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우

5) 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

6) 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우

7) 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

개인정보 유출 통지시 통지 내용

1) 유출된 개인정보의 항목

2) 유출된 시점과 경위

3) 정보주체가 할 수 있는 피해 최소화 방법

4) 개인정보처리자의 대응조치 및 피해 구제절차

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

개인정보 유출 신고 대상

1) 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우

2) 민감정보 또는 고유식별정보가 유출된 경우

3) 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출된 경우

정보보호 대책 분류

<유형에 따른 분류>

1) 기술적 보호대책 : 시스템, 네트워크, 애플리케이션, 정보 등을 보호하기 위한 가장 기본적인 보호대책으로 정보보호 솔루션(하드웨어, 소프트웨어) 도입, 접근통제, 암호 기술, 백업 체계, 보안성이 강화된 시스템등

2) 관리적 보호대책 : 정보보호를 계획하고, 설계하고, 관리하기 위한 정보보호정책, 표준, 지침, 절차 및 정보보호 조직의 구성 등이 해당

<통제 성격에 따른 분류>

1) 예방 통제 : 발생할 수 있는 위험을 식별하여 사전에 대처하는 능동적 개념의 통제
   - 물리적 접근통제 : 비인가자가 물리적 시설이나 설비에 접근할 수 없도록 하는 각종 통제
   - 논리적 접근통제 : 비인가자가 정보통신망을 통해 자산에 접근할 수 없도록 하는 각종 통제
2) 탐지 통제 : 예방 통제를 우회하여 발생하는 각종 위험을 탐지하는 통제
3) 교정 통제 : 탐지된 위협에 대처하거나 감소시키는 통제

정보거버넌스

최고 경영층 및 이사회의 정보보호 프로그램에 대한 지시 및 통제 활동과 이를 위한 조직, 역할과 책임, 절차등을 포함

<정보거버넌스의 3대 목표 ABC>

1) 책임성(Accountability)
  - 정보보호는 다양한 이해관계자들의 요구를 만족시켜야 하며 이사회와 최고경영자의 정보보호 활동에 대한 역할과 책임이 명시되어야 한다
2) 비즈니스 연계성(Business Alignment)
  - 정보보호는 비즈니스 목표 및 전략과 연계되어야 하고 이를 기반으로 정보보호 투자를 정당화한다
3) 준거성(Compliance0
  - 정보보호 요구사항은 조직 내부 요구사항과 외부의 관련법과 규정을 준수해야 하고 이에 대한 검토와 평가가 이루어져야 한다

RAID

데이터 중복 지원 시스템의 대표적인 방법 / 이중화 및 성능향상을 위한 기술

몇 개의 물리적인 디스크를 묶고 이것들을 논리적 배열로 정의하여 실제 데이터는 여러 개의 물리적인 디스크에 저장

-> 저가의 디스크들을 배열 구조로 중복으로 구성함으로써 대형 디스크 장비에 버금가는 성능과 가용성 및 안전한 복구 기능을 제공

주요정보통신기반시설의 지정시 고려사항

1) 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2) 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3) 다른 정보통신기반시설과의 상호연계성
4) 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5) 침해사고의 발생가능성 또는 그 복구의 용이성

개인정보 처리방침에 포함되어야 할 사항

1) 개인정보의 처리 목적
2) 개인정보의 처리 및 보유기간
3) 개인정보의 제3자 제공에 관한 사항(해당시)
4) 개인정보의 파기절차 및 파기방법
5) 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당시)

6) 개인정보처리의 위탁에 관한 사항(해당시)
7) 가명정보의 처리 등에 관한 사항(해당시)
8) 정보주체와 법정대리인의 권리/의무 및 그 행사방법에 관한 사항
9) 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
10) 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치/운영 및 그 거부에 관한 사항(해당시)
11) 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항 - 처리하는 개인정보의 항목
- 개인정보의 안전성 확보 조치에 관한 사항
개인정보 처리방침의 공개 방법
1) 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재
2) 개인정보처리자의 사업장 등의 보기 쉬운 장소에 게시
3) 관보나 해당 지역을 주된 보급지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷 신문에 싣는 방법
4) 같은 제목으로 연 2회이상 발행하여 정보주체에게 배포하는 간행물/소식지/홍보지 또는 청구서 등에 지속적으로 싣는 방법
5) 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법
침해사고 대응 절차
1) 사고 전 준비 : 사고가 발생하기 전 침해사고 대응팀(CERT)과 조직적인 대응 준비
2) 사고 탐지 : 정보보호 및 네트워크 장비에 의한 이상 징후 탐지, 관리자에 의한 침해사고의 식별
3) 초기 대응 : 초기 사고 수행, 사고 정황에 대한 기본적인 세부 사항 기록, 침해사고 대응팀 신고 및 소집, 침해사고 관련 부서에 통지
여부를 판단
5) 사고 조사 : 데이터 수집 및 분석을 통해 사고 조사를 수행하여 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정
6) 보고서 작성 : 의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서를 작성
7) 해결 : 차기 유사 공격을 식별 및 예방하기 위한 보안 정책의 수립, 절차 변경, 사건의 기록, 장기 보안 정책 수립, 기술 수정 계획 수립등을 결정
고정형 영상정보처리기기의 설치,운영 시 안내판에 포함되어야 하는 사항
1) 설치 목적 및 장소
2) 촬영 범위 및 시간
3) 관리책임자의 성명 및 연락처
4) 그 밖에 대통령령으로 정하는 사항
법률의 정식 명칭
국민 생활의 향상과 공공복리의 증진에 이바지하는 것을 목적

안전과 국민생활의 안정을 보장하는 것을 목적

생활의 향상과 공공복리의 증진에 이바지함을 목적

개인정보 가명처리 단계

1) 목적 설정 등 사전 준비 : 가명처리 목적 설정, 처리대상 선정, 목적 적합성 검토, 안전조치, 서류작성 등의 단계를 거친다

2) 위험성 검토 : 대상 선정, 식별 위험성 검토, 이용/제공에 따른 검토를 진행

3) 가명처리 : 항목별 가명처리 계획을 설정하고 가명처리를 수행

4) 적정성 검토 : 필요서류, 목적 적합성, 식별 위험성, 가명처리 방법/수준, 가명처리, 목적 달성 가능성 등의 다양한 부분에서 적정성을 검토 과정을 거친다

5) 안전한 관리 : 재식별 금지, 재식별 가능성 모니터링, 안전조치 시행, 가명정보 처리기록작성/보관 등의 과정을 거친다

* 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존등을 위하여 정보주체의 동의없이 가명정보를 처리할 수 있다

개인정보 가명/익명 처리를 위해 사용하는 기술 중 일반화 기술(범주화 : 특정한 값을 상위 속성으로 대체)

1) 라운딩

- 일반 라운딩 : 올림, 내림, 반올림 등의 기준을 적용하여 집계 처리하는 방법
- 랜덤 라운딩 : 수치 데이터를 임의의 수인 자릿수, 실제 수 기준으로 올림 또는 내림하는 기법
- 제어 라운딩 : 라운딩 적용 시 값의 변결에 따라 행이나 열의 합이 원본의 행이나 열의 합과 일치하지 않는 단점을 해결하기 위해 원본과 결과가 동일하도록 라운딩

2) 상하단 코딩

- 정규분포의 특성을 가진 데이터에서 양쪽 끝에 치우친 정보는 적은 수의 분포를 가지게 되어 식별성을 가질수 있다
- 이를 해결하기위해 적은 수의 분포를 가진 양 끝단의 정보를 점주화 등의 기법을 적용하여 식별성을 낮추는 기법

3) 로컬 일반화

- 전제 정보 집합물 중 특정 열 항목에서 특이한 값을 가지거나 분포상의 특이성으로 인해 식별성이 높아지는 경우 해당 부분만 일반화를 적용하여 식별성을 낮추는

4) 범위 방법

- 수치 데이터를 임의의 수 기준의 범위로 설정하는 기법으로, 해당 값의 범위 또는 구간으로 표현

5) 문자데이터 범주화

- 문자로 저장된 정보에 대해 보다 상위 개념으로 범주화하는 기법

대상별 안전성 기준 및 암호 알고리즘

1) 비밀번호

- 복호화되지 않도록 안전한 일방향 암호 알고리즘(해시함수)을 사용하여 암호화한다
- 주요 권장 일방향 암호 알고리즘에는 SHA-256/384/512등이 있으며 암호화시 솔츠, 반복횟수등을 추가하여 암호강도를 높이도록 한다

2) 고유식별번호, 신용카드번호, 계좌번호, 생체인식정보

- 안전한 암호 알고리즘(대칭키 또는 공개키 암호 알고리즘)을 사용하여 암호화
- 주요 권장 대칭키 암호 알고리즘에는 SEED, ARIA-128/192/256, AES-128/192/256등이 있으며
- 주요 권장 공개키 암호 알고리즘에는 RSA(키 길이 2048bit 이상)이 있다

디지털 포렌식

침해사고(또는 사이버 범죄) 발생 시 법적으로 유효한 증거를 디지털기기로부터 수집하고, 분석하고, 보관하고, 제출하는 등의 일련의 과정을 다루는 과학 분야

<기본 5 원칙>

1) 정당성의 원칙 : 디지털 증거를 수집하고 분석하는 전 과정이 적법한 절차에 의해 이루어져야 한다
2) 재현성의 원칙 : 동일한 조건에서 디지털 포렌식을 재현할 경우 항상 동일한 결과가 나와야 한다
3) 무결성의 원칙 : 수집된 디지철 증거가 분석 또는 보관하는 과정에서 위/변조되지 않아야 한다
4) 신속성의 원칙 : 디지털 데이터는 내/외부 영향에 의해 쉽게 사라질 수 있으므로 디지털 포렌식은 가능하면 신속하게 진행되어야 한다
5) 연계 보관성 원칙 : 디지털 증거의 '수집(획득)-이송-보관-분석-법정 제출'까지의 일련의 단계에서 증거물 관리 주체간의 연속적인 승계 내역을 기록함으로써 디지털

데이터 분석(포렌식 분석)

모든 수집된 정보의 전체적 조사를 의미하며 소프트웨어 분석, 시간/날짜 스탬프 분석, 키워드 검색, 그 외의 필요한 조사과정을 수행한다

<분석할 정보>

- 로그파일
- 시스템 설정 파일
- 웹 브라우저 히스토리 파일
- 이메일 메시지와 첨부파일
- 설치된 애플리케이션
- 그림 파일 등

ISPS-P인증기준

1) 관리체계 수립 및 운영

- 관리체계 기반 마련
- 위험 관리
- 관리체계 운영
- 관리체계 점검 및 개선

2) 보호대책 요구사항
- 정책, 조직, 자산 관리
- 인적 보안
- 외부자 보안
- 물리 보안
- 인증 및 권한 관리
- 접근 통제
- 암호화 적용
- 정보시스템 도입 및 개발 보안
- 시스템 및 서비스 운영관리
- 시스템 및 서비스 보안관리
- 사고 예방 및 대응

3) 개인정보 처리 관계를 요구사항
- 개인정보 수집 시 보호조치
- 개인정보 보유 및 이용 시 보호조치
- 개인정보 제공 시 보호조치
- 개인정보 파기 시 보호조치
- 정보주체 권리보호

위험 평가서

식별된 자산에 위험 발생시의 영향을 기밀성, 무결성, 가용성 측면에서 파악하여 자산의 가치와 위험도를 평가하기 위함

우려사항 : 위협과 취약성을 통합하여 정의한 함목으로 위협과 취약성이 서로 밀접하게 연관되어 있고 구분하기 어려운 경우 우려사항 항목으로 통합하여 정의

가능성 : 우려사항의 평가 기준으로 우려사항이 발생하여 자산에 영향을 미칠 가능성을 의미

용어

DMZ 구간 : 내부 시스템 및 네트워크를 보호하기 위한 보안층 역할
: 외부에서 인터넷을 통해 직접 접근해야 하는 웹 서버, 메일 서버, DNS 서버 등 공개 서버들이 DMZ 구간에 위치하며 외부에서 직접 접근이 줄핑요한 웹 애

정보보호 관리체계(ISMS)
- 조직의 정보자산의 무결성, 기밀성, 가용성 등을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리, 운영하는 체계로 조직의적절한 정보보호를 위해 정보보호 관리 과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계를 의미

정보통신기반 보호법 : 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립/시행함으로써 동 시설을 안정작으로 운영하도록 하여 국가의 안

정보보호 사전점검 : 정보통신망의 구축 또는 정보통신서비스의 제공 이전에 계획 또는 설계등의 과정에서 정보보호를 고려하여 필요한 조치를 하거나 계획을 마련하는