개인정보 위험도 분석 기준 및 해설서

2012. 3.

행정안전부

KISA 한국인터넷진흥원
Korea Internet & Security Agency

◎ 본 해설서는 「개인정보보호법」 제29조 및 「개인정보의 안전성 확보조치 기준」에 따라 고유식별정보 내부망 저장시 암호화의 적용여부 및 적용범위 결정을 위한 「위험도 분석」의 세부 기준 제시를 목적으로 합니다.

목 차

Ⅰ 개요

1. 추진 근거

■ 「**개인정보보호법**」 제29조 및 「**개인정보의 안전성 확보조치 기준**」 제7조 5항에 따라 개인정보처리자가 **내부망**에 **고유식별정보**를 저장하는 경우, 「**위험도 분석 기준**」 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있습니다.

■ 개인정보처리자는 개인정보 영향평가 또는 위험도 분석에 따른 결과에 따라 **2012년 12월 31일까지 암호화 기술의 적용 또는 이에 상응하는 조치**를 완료해야 합니다.

※ 개인정보 영향평가 : 개인정보보호법 제33조, 시행령 38조, 개인정보 영향평가에 관한 고시 참조

2. 위험도 분석 기준이란?

■ 위험도분석은 개인정보처리시스템에 적용하고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 침해할 위험의 정도를 「**위험도 분석 기준**」을 이용하여 분석하는 행위입니다.

■ 「**위험도 분석 기준**」은 내부망에 고유식별정보를 암호화하지 않고 저장하는 경우 개인정보처리자가 이행하여야 할 최소한의 보호조치 기준으로 어느 하나의 항목이라도 **'아니오'**에 해당하는 경우 **암호화 대상**입니다.

※ 해당사항이 없는 경우 '해당없음' 항목에 체크하며 '해당없음' 체크항목도 '예'로 적용합니다.

■ 개인정보처리자는 「**위험도 분석 기준**」을 허위로 작성해서는 안되며, 「위험도 분석 결과보고서」는 개인정보 보호책임자 또는 해당 부서의 장의 결재를 득한 후 보관합니다.

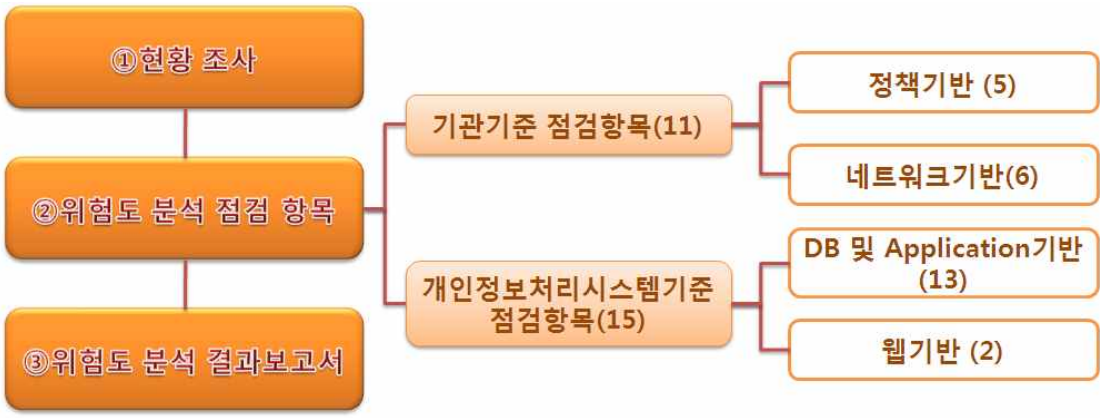
■ 「**위험도 분석**」은 개인정보파일 단위로 분석하고 결과보고서를 작성하며, 개인정보파일을 위탁한 경우에도 위탁기관이 작성합니다.

※ 결과보고서는 기관의 문서관리 규정에 따라 '대외비' 등으로 관리하시기 바랍니다.

■ 「**위험도 분석**」은 최초 분석 이후에도 개인정보처리시스템을 증설하거나, 내·외부망과 연계하거나, 기타 운영환경이 변경된 경우에도 지속적으로 실시하여야 합니다.

3. 위험도 분석 기준 구성

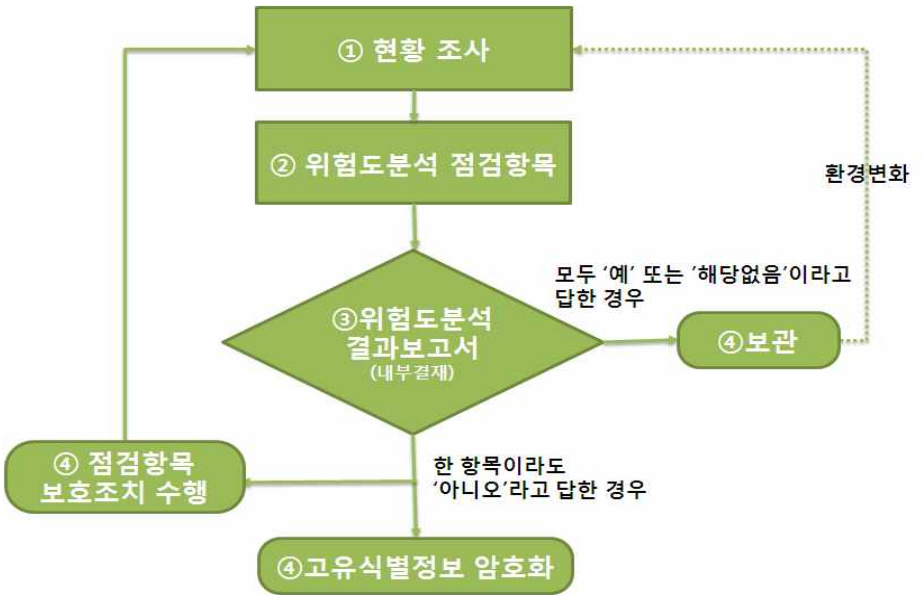
■ 위험도 분석 기준은 ①현황 조사, ②위험도 분석 점검 항목, ③위험도 분석 결과 보고서로 구성되어 있습니다.



[그림 1] 위험도 분석 기준 구성

4. 위험도 분석 절차

① 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사
② 개인정보 파일단위별로 위험도 분석 항목별 점검을 수행
③ 위험도 분석 결과보고서를 작성하여 내부결재 후 보관
④ 점검 결과에 따라 고유식별정보 암호화 등을 수행



[그림 2] 위험도 분석 절차

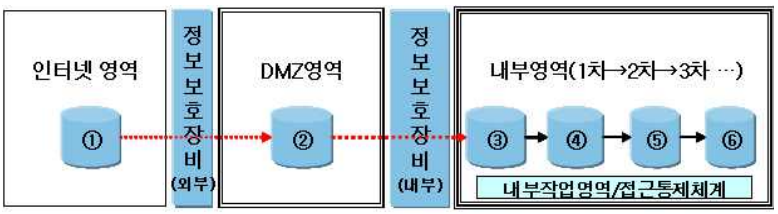
Ⅱ 위험도 분석 기준

1. 현황 조사

① 개인정보 파일 현황

개인정보 파일 명칭	취급개인정보	네트워크 연결여부 (개인정보파일 연동사용)	보유량 (단위:만건)	개인정보 처리시스템명
개인정보파일_1	(예시)이름, 전화번호, 주소	(예시)인터넷으로 지점 연동 (서울 ↔ 인천)	10	고객관리시스템
개인정보파일_2	(예시)이름, 전화번호, 이메일, 주민등록번호 등	(예시) OOO 업체와 개인정보파일 연동	500	교육비정산시스템
개인정보파일_3	(예시)이름, 발행일, 여권번호	(예시) OOO 행정기관과 개인정보파일 연동	1,000	여행사 업무시스템
…				
개인정보파일_n				

② 고유식별정보 현황

점 검 항 목	비 고
1. 취급하는 고유식별정보에 해당되는 항목을 모두 체크하여 주십시오. ① 주민등록번호 ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호	o ①~④번 항목에 해당사항이 없을 경우 고유식별정보 암호화 의무 대상이 아닙니다.
2. 1번 항목에서 취급하는 개인정보를 어떻게 저장하고 있습니까? ① 모든 항목 암호화 저장 ② 일부 항목 암호화 저장 ③ 암호화 하지 않고 저장	o ①번 항목 선택 시에는 이미 암호화 중이므로 위험도 분석을 할 필요가 없습니다.
3. 개인정보파일의 저장위치는 어디 입니까? ① 인터넷 영역 ② DMZ영역 ③ 내부영역(업무망) ※ 아래 그림을 참고하여 해당 개인정보의 저장·검색·편집·정정 등을 위한 개인정보처리시스템(DB 등)이 위치하고 있는 번호에 체크하십시오. 	o ①번 또는 ②번 항목 선택 시 위험도 분석 점검표와 관계없이 암호화 대상입니다.

2. 위험도 분석 점검 항목

① (기관 기준) 점검 항목

※ 개인정보 파일이 포함되어 있는 개인정보처리시스템 환경에 관한 내용으로 기관 전체를 대상으로 합니다.

구 분	점 검 항 목	예	아니오	해당없음
정책기반	1. 개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?			
	2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?			
	3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?			
	4. DB 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립·운영하고 있습니까?			
	5. DB서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시하고 있습니까?			
네트워크 기반	6. 상시적으로 비인가 IP주소의 접근을 통제하고 있습니까?			
	7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?			
	8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?			
	9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?			
	10. 주기적으로 네트워크 접속에 대한 로그를 관리하고, 분석하고 있습니까?			
	11. 네트워크 장비 및 정보보호시스템의 보안패치 발생시 지체없이 업데이트를 수행하고 있습니까?			

② (개인정보처리시스템 기준) 점검 항목

※ 개인정보파일이 운용되는 개인정보처리시스템의 보호조치에 관한 내용입니다.

구 분	점 검 항 목	예	아니오	해당없음
DB 및 Application 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?			
	13. DB서버내에 불필요한 서비스 포트를 차단하고 있습니까?			
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?			
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?			
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?			
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?			
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동 발생시 지체없이 DB 접근권한을 변경하고 있습니까?			
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?			
	20. DB접속자 및 개인정보취급자의 비밀번호 입력시 5회 이상 연속 입력오류가 발생한 경우 계정잠금 등 접근을 제한하고 있습니까?			
	21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?			
	22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용시 관리자 승인 후 사용하고 있습니까?			

구 분	점 검 항 목	예	아니오	해당없음
	23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?			
	24. HDD등 DB 저장매체의 불용처리시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?			
웹(Web) 기반 ※ 웹사이트를 운영하는 경우에만 해당	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?			
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?			

3. 위험도 분석 결과보고서

작성일	년 월 일	작성자	(소속)	(성명)
개인정보파일명				

(작성 예시)

< 목 차 >

Ⅲ 위험도 분석 기준 해설

1. 현황 조사

1-1. 개인정보 파일 현황

개인정보 파일 명칭	취급개인정보	네트워크 연결여부 (개인정보파일 연동사용)	보유량 (단위:만건)	개인정보 처리시스템명
개인정보파일_1	(예시)이름, 전화번호, 주소	(예시)인터넷으로 지점 연동 (서울 ↔ 인천)	10	고객관리시스템
…				
개인정보파일_n				

해 설

■ 「개인정보 파일 현황」은 개인정보처리시스템을 기준으로 해당 시스템이 보유하고 있는 개인정보 파일 목록을 기재합니다.

■ 각 개인정보파일별 취급하는 개인정보항목, 네트워크 연결여부, 개인정보 보유량 등을 기재하고 해당 개인정보 파일이 운영되고 있는 개인정보처리시스템명을 기재합니다.

■ 위험도 분석 점검의 단위인 '개인정보파일'이란 반드시 DB테이블 단위로 구분되는 것은 아닙니다. 업무단위 또는 정보시스템의 기능 목록명 또는 프로세스명으로 분류하여 고유식별정보를 저장하는 DB테이블을 통합하여 점검 가능합니다.

- '개인정보파일'의 의미

정 의 '개인정보파일'이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

【예시】'○○ e-러닝시스템'이란 시스템이 있다면, 강사목록 테이블, 수강생목록 테이블 등을 교육관리라는 업무로 분류하여 위험도 분석을 할 수 있습니다.

2-1. 고유식별정보 현황

1. 취급하는 고유식별정보에 해당되는 항목을 모두 체크하여 주십시오.
① 주민등록번호 ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호

해 설

- 위험도 분석은 내부망에 고유식별정보를 저장할 경우의 암호화 여부를 결정하는 기준이므로 해당 개인정보파일에서 고유식별정보를 처리하고 있는지 점검하여 체크합니다.
- 해당사항이 없을 경우 고유식별정보 암호화 의무 대상이 아니므로 위험도 분석을 중단할 수 있습니다.

2. 1번 항목에서 취급하는 개인정보를 어떻게 저장하고 있습니까?
① 모든 항목 암호화 저장 ② 일부 항목 암호화 저장 ③ 암호화 하지 않고 저장

해 설

- ①번 : 해당 개인정보파일에서 처리하고 있는 모든 고유식별정보를 암호화하여 저장하는 경우 선택

  ②번 : 여러 고유식별정보 중 일부 항목만 암호화하여 저장하는 경우 선택

  ③번 : 모든 고유식별정보를 암호화 하지 않고 저장하는 경우 선택

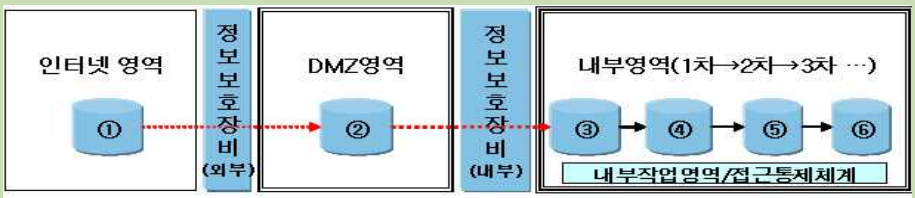
- ①번 항목 선택시 모두 암호화 중이므로 위험도 분석을 수행할 필요가 없습니다. 암호화 저장의 의미는 다음 암호화 범위와 강도를 참조합니다.
- 암호화의 범위
  - 고유식별정보는 원칙적으로 모든 자리수를 암호화해야 하나, 주민등록번호를 자료 검색키로 사용하는 경우 암호화/복호화에 대한 부하가 발생할 수 있으므로, 속도 등 성능을 고려하여 최소한의 정보만 평문으로 저장하고 이외의 정보를 암호화하는 부분 암호화 조치를 취할 수 있습니다.
  - 주민등록번호는 생년월일과 성별정보를 포함하고 있는 앞 7자리를 제외한 뒷자리 6개 번호 이상 암호화하는 것이 바람직합니다.
    【예시】700101-1#....&
  - 여권번호, 운전면허번호, 외국인등록번호는 모든 자리수를 암호화해야 합니다.

■ 암호화의 강도

- 암호화는 안전한 암호 알고리즘으로 수행되어야 하며, 이는 미국 NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 기관 및 국내외 암호 연구기관에서 권고하는 알고리즘을 의미합니다.

3. 개인정보파일의 저장위치는 어디 입니까?
① 인터넷 영역 ② DMZ 영역 ③ 내부망 영역(업무망)

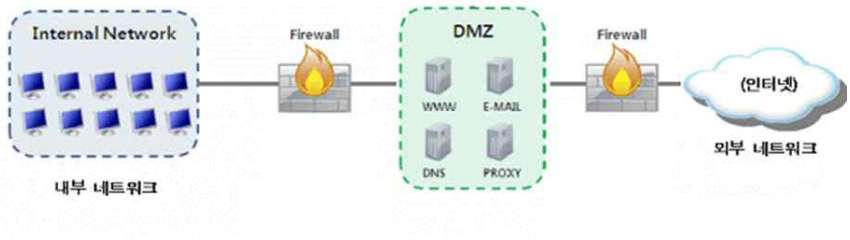
※ 아래 그림을 참고하여 해당 개인정보의 저장·검색·편집·정정 등을 위한 개인정보처리 시스템(DB 등)이 위치하고 있는 번호에 체크하십시오.



해 설

■ 용어 정의

- 인터넷 영역 : 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간입니다.
- DMZ 영역 : 인터넷 구간과 내부망 구간 사이에 위치한 중간 지점으로 침입차단 시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말합니다.
- 내부망 영역 : 접근통제시스템등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역을 말합니다.



[그림 3] 네트워크 구성도

■ ①번 또는 ②번 항목 선택시 위험도분석과 상관없이 무조건 암호화 대상입니다. 인터넷 영역이나 DMZ 영역은 외부에서 직접 접근이 가능하므로 외부 침입의 위험성이 크기 때문에 이 영역에 고유식별정보를 저장하려는 경우 반드시 암호화해야 합니다.

2. 위험도 분석 점검 항목

2-1. (기관 기준) 점검 항목

2-1-1 정책기반

1. 개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?

취 지

■ 개인정보 보호책임자를 지정하는 것은 형식적인 절차가 아닌 개인정보처리자의 내부관리체계를 강화하고, 개인정보의 안전한 관리가 가능하도록 하는 취지입니다. 이를 위해 전문지식을 보유하고 보호조치 수행이 가능한 개인정보 보호책임자를 지정하여 운영합니다.

해 설

■ 개인정보보호법 제31조 1항 및 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자(CPO : Chief Privacy Officer)를 지정해야 합니다.

참 고

■ 개인정보 보호책임자는 상당한 개인정보 관련 업무경력과 개인정보 관련 전문지식을 모두 보유한 사람으로 개인정보 처리업무를 자신의 책임하에 관리할 수 있는 직위를 가져야 합니다.(자세한 자격요건은 시행령 제32조 참조)

- 개인정보 보호책임자는 개인정보처리에 관한 전반적인 사항을 결정하고 이로 인한 제반 결과에 대하여 책임을 지는 자이므로 개인정보 수집·이용·제공 등에 대하여 실질적인 권한을 가지고 있어야 합니다.

- 개인정보 처리업무 경험이 있는 자로서, 개인정보보호를 위한 관리적·기술적·물리적 보호조치를 할 수 있는 사람이어야 합니다.

■ 개인정보 보호책임자가 실무를 담당하지 않는 경우, 개인정보의 기술적·관리적·물리적 조치를 실행할 수 있는 개인정보 보호담당자를 지정하여 업무를 수행합니다.

■ 개인정보 책임자의 지정, 역할, 책임에 관한 내용은 내부관리계획 등에 명시하여 최고경영층으로부터 승인받습니다.

■ 개인정보 보호책임자 및 보호담당자는 개인정보관리책임자(정보통신망법), 신용정보 보호책임자(신용정보법), 정보보호(Security) 등 다른 업무와 겸직이 가능하지만 개인정보보호법상 규정 업무를 모두 수행합니다.

※ 개인정보 보호책임자가 다른 업무와 겸직하는 경우 반드시 업무시간의 일부를 개인정보 보호에 할애하는 등 개인정보보호 업무를 실제로 수행하여야 합니다.

■ 조직도, 책임자, 역할 및 책임 등이 명시된 증적자료를 위험도 분석 결과보고서에 첨부합니다.

2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?

취 지

■ 개인정보보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으므로 당해 조직의 구성원 전체에 통용되는 내부 규정을 마련합니다.

해 설

■ 개인정보 보호를 위한 정책 또는 관리계획이라 함은 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립·시행하는 내부 기준으로 내부관리계획, 개인정보보호 추진계획, 개인정보보호 관련 각종 내부지침 의미합니다.

■ 특히, 개인정보 침해사고에 대비하여 침해사고시 대응 절차, 담당자, 피해복구조치 등 침해 대응 계획이 포함되어야 합니다.

■ 개인정보보호 정책 및 침해사고 대응계획 수립현황 등 증적자료를 위험도 분석 결과보고서에 첨부합니다.

3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?

취 지

■ 조직에서 구성원들의 개인정보 유출 위험을 최소화하고, 구성원에게 개인정보보호에 대한 책임을 명확히 주지시키기 위해 문서화한 보안서약서에 서명하도록 해야 하며,

개인정보를 취급하는 외주 인력도 보안관리 대상에서 제외되지 않도록 합니다.

해설

- '개인정보취급자'는 기업·단체·공공기관의 임직원, 계약직원, 아르바이트 직원 등의 시간제 근로자뿐만 아니라 외부기관에서 또는 외부기관으로 파견된 근로자 등도 해당됩니다.
- 최근의 개인정보 유출사례를 보면 개인정보취급자에 대한 관리 소홀, 특히 외주 인력에 대한 보안관리 소홀이 그 원인이 되는 경우가 많으므로 보안서약서 집행, 비밀번호 노출 예방 등 외주 인력의 보안관리 조치를 수행하여 개인정보 유출을 방지합니다.
- 외주 보안관리 현황 등 증적자료를 위험도 분석 결과보고서에 첨부합니다.

4. DB서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립·운영하고 있습니까?

취 지

- 불법 S/W 사용은 악성코드 침투 경로로 이용되어 악성코드에 의한 개인정보 유출사고가 발생할 수 있습니다. 따라서 개인정보의 안전한 관리를 위하여 정품 S/W를 사용합니다.

해설

- 운영체제 S/W의 경우, 불법복제 S/W는 정품 인증을 받지 못함에 따라 신규 보안 위협 제거를 위한 업데이트 지원을 받지 못하게 되어 운영체제 취약점을 이용한 악성코드 감염으로 대량의 개인정보 유출 피해가 발생할 수 있습니다. 따라서 DB서버에 접속하는 장비 또는 개인정보취급자의 PC에는 정품 S/W만을 사용하도록 하는 정책을 수립합니다.
- S/W 사용정책 및 현황 등 증적자료를 위험도 분석 결과보고서에 첨부합니다.

5. DB서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시하고 있습니까?

취 지

- 개인정보처리자는 개인정보취급자의 개인정보보호에 대한 인식을 제고시키기 위해 매년 정기적으로 개인정보보호 교육을 실시합니다.
- 특히 고유식별정보가 저장된 DB서버에 접근 가능한 자에 대해서는 최소 연2회 이상 교육을 실시합니다.

해 설

- 최근의 유출사례에서 볼 수 있듯이 개인정보 유출은 내부직원의 보안의식 부재에 의한 경우가 많기 때문에 개인정보취급자에 대한 연 2회 이상의 교육을 실시합니다.
  - 사례 1) A사 내부 직원이 고객정보를 출력물로 유출
  - 사례 2) C사 직원 실수로 고객정보 포함된 이메일 발송

참 고

■ 개인정보취급자

- 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자 와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자 (표준지침)

- 개인정보취급자는 개인정보 처리 업무를 담당하고 있는 자라면, 정규직, 비정규직, 하도급, 시간제 등 모든 근로 형태를 불문합니다. 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함된다.(개인정보 보호법령 및 지침·고시 해설서)

- 정기적인 개인정보취급자 교육을 통해 안전하게 개인정보가 관리될 수 있도록 개인정보취급자의 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시킵니다.

- 교육방법은 집체교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문인력에 위탁하여 교육을 실시할 수 있습니다.

※「일일 업무 회의시 과내 약식으로 수행되는 전달교육」 등은 개인정보보호 교육에 해당하지 않으며 반드시 독립된 교육과정 또는 교과목으로 수행되어야 합니다.

- 교육내용에는 업무를 수행함에 있어 필요한 개인정보 관련 기술교육 뿐만 아니라 개인 정보보호 관련 법률 및 제도, 사내 규정 등 필히 알고 있어야 하는 기본적인 내용을 포함하여 교육을 실시합니다.

참 고

■ **개인정보보호 교육내용 예시**

- 개인정보보호의 중요성 설명
- 내부관리계획의 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법
- 개인정보의 기술적·관리적 보호조치 기준 이행
- 개인정보보호 위반을 보고해야 할 필요성
- 개인정보보호업무의 절차, 책임, 작업 설명
- 개인정보보호 관련자들의 금지 항목들
- 개인정보보호 준수사항 이행 관련 절차 등

■ 교육 목적, 대상, 내용, 일정 및 방법 등을 포함하는 'OO년 개인정보보호 교육계획', 교육결과보고 등 증적자료를 위험도 분석 결과보고서에 첨부합니다.

2-1-2 N/W기반

6. 상시적으로 비인가 IP주소의 접근을 통제하고 있습니까?

취 지

■ IP 접근통제의 목적은 개인정보처리시스템에 대해 인가되지 않는 접근을 차단하여 개인정보의 불법사용, 누출, 변조, 훼손 등의 위험을 적절히 차단하는 것입니다.

해 설

■ 침입차단시스템(Firewall) 또는 침입방지시스템(IPS : Intrusion Prevention System) 등의 설치·운영을 통해 불법적인 접근을 IP주소 등으로 제한할 수 있으며 개인정보처리시스템에 대한 불법적인 개인정보 유출시도를 탐지합니다.

■ IP 접근통제 현황을 위험도 분석 결과보고서에 첨부합니다.

7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?

취 지

■ 서비스와 상관없는 포트가 불필요하게 개방되어 있는 경우 불법 침입의 경로로 이용될 수 있으므로 서비스에 꼭 필요한 포트만 사용하도록 통제합니다.

해 설

■ 불필요한 서비스 포트는 침입차단시스템(Firewall), 서버 설정 등으로 차단, 악성코드 유입 및 불법 침입 경로를 차단합니다.

■ 서비스 포트 제한 현황 등을 위험도 분석 결과보고서에 첨부합니다.

8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?

취 지

■ 침입차단시스템 및 침입탐지 기능을 갖춘 설비를 설치해야 하는 것은 물론이고, 이에 대한 상시 모니터링이 함께 이루어져야 불법적인 해킹시도에 대한 대응이 가능합니다.

해 설

■ IDS, IPS등 정보보호시스템을 갖추고, 모니터링을 수행하여 불법적인 해킹시도를 상시 방지합니다.

■ 정보보호시스템 운영 모니터링 현황을 위험도 분석 결과보고서에 첨부합니다.

9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?

취 지

- 바이러스, 웜 등 악성 프로그램들이 네트워크를 통해 유입되어 감염될 경우 해킹에 의한 개인정보 유출의 통로로 이용될 수 있으므로 네트워크 상에서 상시적으로 악성 프로그램 검사를 수행하여 유입을 차단합니다.

해 설

- 네트워크를 통해 유입되는 콘텐츠의 바이러스 감염 여부를 검사하고 차단 및 치료할 수 있는 바이러스 방지 솔루션을 설치·운영합니다.
- 네트워크 바이러스 차단 현황 등을 위험도 분석 결과보고서에 첨부합니다.

10. 주기적으로 네트워크 접속에 대한 로그를 기록·백업하고, 주기적으로 분석하고 있습니까?

취 지

- 네트워크 접속 로그 파일을 생성함으로써 불법적인 접근 및 행위를 확인 가능하고 유출사고 발생시 책임추적성을 확보할 수 있습니다.

해 설

- access log 등을 기록·백업하고 주기적으로 분석하여 이상 징후를 파악하고 대응합니다.
- 네트워크 접속기록 관리 및 분석 현황 등을 위험도 분석 결과보고서에 첨부합니다.

11. 네트워크 장비 및 정보보호시스템의 보안패치 발생시 지체없이 업데이트를 수행하고 있습니까?

취 지

- 네트워크 장비, 정보보호시스템은 항상 최신 업데이트를 유지하여 신규로 발생하는 보안 위협에 대응합니다.

해 설

- 라우터, 스위치 등 네트워크 장비 및 Firewall, VPN, IPS 등 정보보호시스템 운영시 환경설정, 보안정책 설정, 침입패턴 등을 최신으로 유지할 수 있도록 업데이트를 수행하고 취약점 발견 등으로 인한 보안패치 발생시 업데이트를 수행합니다.
- '지체없이'란 현재 운영중인 응용프로그램과의 업무연속성, 시스템에 미칠 영향 등을 고려하여 적용하기 까지 소요되는 합리적인 상당시간을 의미합니다.
- 네트워크 장비 및 정보보호시스템 업데이트 현황을 위험도 분석 결과보고서에 첨부합니다.

2-2. (개인정보처리시스템 기준) 점검 항목

2-2-1 DB 및 Application 기반

12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?

취 지

- 방화벽 등 네트워크 단의 침입방지시스템이 잘 운용되고 있는 상황이라도 DB에 대한 비인가자의 접근통제는 별도로 실시합니다.

해 설

- 상시적으로 DB 접속자 개개인을 식별하여 비인가자에 대한 DB접근을 통제하기 위하여 DB접근제어 솔루션 등을 이용할 수 있습니다.
- 사용자가 DBMS에 로그인하거나 SQL을 수행하려고할 때 미리 정의된 규칙에 따라 권한 여부를 판단하여 통제합니다.
- DB접근통제 현황을 위험도 분석 보고서에 첨부합니다.

13. DB서버 내에 불필요한 서비스 포트를 차단하고 있습니까?

취 지

- 서비스와 상관없는 포트가 불필요하게 개방되어 있는 경우 불법 침입의 경로로 이용될 수 있으므로 서비스에 꼭 필요한 포트만 사용하도록 통제합니다.

해 설

- 관리자가 DB관리를 위해 사용해야하는 포트, 어플리케이션 서버에서 DB연결을 위해 필요한 포트 등 꼭 필요한 포트 이외는 차단하여 악성코드 유입 및 불법 침입 경로를 차단합니다.
- 서비스 포트 제한 현황 등을 위험도 분석 결과보고서에 첨부합니다.

14. 상시적으로 DB 관리자 및 개인정보취급자의 접속기록을 남기고 있습니까?

취 지

- DB 접속 및 개인정보 처리내역 등을 자동으로 기록하는 로그 파일을 생성함으로써 불법적인 접근 및 행위를 확인 가능하고 유출사고 발생시 책임추적성을 확보합니다.

해 설

- 내부관리자가 DB관리툴, Telnet등을 이용해 DB에 직접 접속하는 경우와 개인정보취급자가 Web 또는 응용프로그램을 통해 접속하는 경우 모두 접속기록을 남겨야 합니다.
- DB 접속기록 관리 현황을 위험도 분석 결과보고서에 첨부합니다.

15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?

취 지

- DB접속기록에 대한 모니터링 과정 없이 단순히 DB접속기록을 남기는 것만으로는 DB접속자의 행위에 대한 효과적인 통제가 이루어진다고 할 수 없습니다. 접속기록의 주기적인 모니터링을 실시하면 DB접속에 대한 이상 징후를 파악하여 조치가 가능하고, DB에 접속하는 모든 사람에게 모니터링이 이루어지고 있음을 인지시킴으로써 불법적인 시도 자체를 줄일 수 있습니다.

해 설

- 매주 DB 접속에 대한 이상 징후가 있는지 DB접속기록에 대해 최소 주 1회 이상 모니터링을 수행합니다.
- DB 접속기록 모니터링 현황을 위험도 분석 결과보고서에 첨부합니다.

16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?

취 지

- 2011년 S업체의 대규모 개인정보 유출사고는 DB관리자의 PC에 악성코드가 삽입되어 DB관리자 계정을 탈취당하여 발생하였습니다.
- 최근의 공격 특성은 회사 홈페이지, 직원들의 SNS에 공개된 정보를 수집하여 사회공학적 공격을 위한 정보 구축 후 수집된 정보를 이용하여 특정 직원에게 악성코드나 악성 링크가 삽입된 이메일을 보내거나 메신저를 통하여 메시지를 전송합니다.
- 위의 유출사례 및 최근 해킹 특성에서 알 수 있듯이 DB 관리자의 PC에서 인터넷 접속이 이루어질 경우 악성 코드에 감염되어 해킹 경로로 이용될 수 있으므로 DB 관리자 PC는 인터넷 접속이 되지 않도록 합니다.

해 설

- DB관리자 PC가 인터넷 접속으로 악성코드에 감염된 채 DB서버에 접속할 수 없도록 DB에 접속하는 DB관리자 PC는 인터넷 접속이 불가능하도록 접속을 차단합니다.
- DB관리자 PC의 망 분리는 네트워크를 별도로 구축하는 물리적 망 분리 외에 가상화를

이용한 논리적 망분리도 가능합니다.

■ DB관리자 PC의 네트워크 분리 현황 등을 위험도 분석 결과보고서에 첨부합니다.

17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?

취 지

■ 접근권한 관리의 목적은 개인정보처리시스템에 대하여 업무 목적 외 불필요한 접근을 차단하여 개인정보의 도난, 유출, 변조, 훼손을 방지하기 위한 것입니다.

해 설

■ 개인정보취급자의 역할에 따라 조회, 등록, 수정, 삭제 등의 권한을 업무수행 목적에 따라 최소한의 범위로 차등화하여 부여합니다.
【사례】 A사 실시간 교통정보 제공 서비스 홈페이지에서 '08년 1년간 휴대폰으로 접속한 고객의 접속기록파일이 권한 없이 조회 가능하여 외부에 노출된 사례가 있습니다.

■ 접근권한은 업무 단위 수준에서 차등화하여 부여하면 됩니다.

【예시】 회계부서는 영업부서 화면에 접근하지 못하도록 권한 부여

■ 개인정보취급자 계정 관리 정책, 권한부여·변경 내역을 위험도 분석 결과보고서에 첨부합니다.

18. 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동 발생시 지체없이 DB 접근권한을 변경하고 있습니까?

취 지

■ 인사이동 등으로 더 이상 개인정보취급자가 아닌 사람이 계속 개인정보처리시스템에 접근가능하다면 업무목적 외 불필요한 접근으로 인해 악의적 사용 및 유출 등의 문제가 발생할 수 있습니다. 개인정보취급자의 역할 변경시 철저한 접근권한 통제가 이루어지도록 합니다.

해 설

- 개인정보취급자의 전보, 이직, 퇴사 등으로 인해 계정의 변경·삭제가 필요한 경우 즉시 계정 삭제 및 패스워드 변경 등 DB 접근권한을 변경합니다.

  【사례】 A사 퇴직직원이 재직시 사용하던 ID, 비밀번호로 개인정보처리시스템에 접근 후 고객명부를 불법 탈취하여 경쟁업체에 고객명부를 판매하였습니다.

- 접근권한 변경시에는 일회성 조치로 제외되는 경우가 생기지 않도록 공식적인 사용자 계정 관리 절차에 따라 통제될 수 있도록 합니다.

- '지체없이'란 조직원의 전보, 이직, 퇴사로 인한 인사 이동 발생 후 접근권한을 변경하기까지 소요되는 합리적인 상당시간을 의미합니다.

- 개인정보취급자 계정 관리 정책, 권한부여·변경 내역을 위험도 분석 결과보고서에 첨부합니다.

19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?

취 지

- 비밀번호를 장기간 사용할 경우, 그만큼 비밀번호 해킹의 가능성도 높아지므로 비밀번호의 유효기간을 설정하여 최소 3개월마다 변경합니다.

해 설

- DB에 직접 접속하는 DB 이용자 계정의 비밀번호 유효기간을 3개월 이하로 설정하여 비밀번호를 변경합니다.

- 개인정보취급자의 개인정보처리시스템 로그인시 유효기간을 설정기능을 두어 3개월 마다 강제 변경합니다.

- DB접속자 및 개인정보취급자의 비밀번호에 대한 점검항목이며 미들웨어 등에서 사용하는 DB 비밀번호는 적용 대상이 아닙니다.

- 비밀번호 관리 정책 및 현황을 증적자료로 위험도 결과 보고서에 첨부합니다.

20. DB접속자 및 개인정보취급자의 비밀번호 입력 시 5회 이상 연속 입력오류가 발생한 경우 계정 잠금 등 접근을 제한하고 있습니까?

취 지

■ DB 이용자 계정과 개인정보취급자의 이용자 계정은 비밀번호 해킹을 통한 개인정보 유출 위협이 발생할 수 있으므로 일정 횟수 이상 연속 입력 오류가 발생한 경우에는 접근을 차단합니다.

해 설

■ 계정 잠금 기능이 제공되지 않는 경우 공격자는 해당 계정의 패스워드를 파악할 때까지 지속적인 Brute force attack을 수행할 수 있습니다.

참 고

■ **Brute force attack (무차별 대입 공격)**

- 성공할 때까지 가능한 모든 조합의 경우의 수를 시도해 원하는 공격을 시도하는 것

(예) Crack 등 소프트웨어를 이용하여 계정에 대한 password를 추측하는 방법

■ DB관리자 등 DB에 직접 접속하는 경우, DBMS의 비밀번호 입력횟수 제한 기능을 사용합니다. 기능을 제공하지 않는 DBMS를 사용하는 경우에 한하여 DB서버의 입력횟수 제한 기능 사용이 가능합니다.

참 고

【예시】

- 오라클, mysql : DBMS의 profile 설정
- SYBASE : 계정생성시 옵션 설정, 명령어를 통한 수정
- 인포믹스, DB2 : DB서버의 설정 기능 사용

■ 계정 잠금에 따라 서비스가 신속히 이루어 질 수 있도록 잠금 해제 절차를 수립합니다.

■ DB접속자 및 개인정보취급자의 비밀번호에 대한 점검항목이며 미들웨어 등에서 사용하는 DB 비밀번호는 적용 대상이 아닙니다.

■ 비밀번호 관리정책 및 현황 등을 증적자료로 위험도 결과 보고서에 첨부합니다.

21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?

취 지

■ 개인정보처리시스템의 서버에 비인가자의 물리적 접근이 가능한 경우, 개인정보의 절도, 파괴 등의 위협이 발생할 수 있으므로 물리적 접근 통제를 실시합니다.

해 설

■ 전산실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우 출입을 통제하는 방법으로 물리적 접근통제 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하는 방법 등이 있습니다.

【예시】전자적 매체 기록방법 : 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입통제장치, 지문 등 바이오정보 기반 출입통제 장치 등
【예시】수기문서 대장 기록방법 : '출입자', '출입일시', '출입목적' 등을 출입관리 대상에 기록

■ DB 서버 및 DB 접속 어플리케이션 서버에 대한 비인가자 접근을 차단하기 위해 접근 통제 절차를 수립·운영하여야 하며, 접근기록을 보관합니다.
【예시】 접근 통제 절차에는 출입증·출입카드 발급절차, 회수절차 등 포함

■ DB 서버 및 DB 접속 어플리케이션 서버를 별도의 전산실에서 운영하지 않는 경우 비인가자의 무단접근하지 못하도록 통제선, 칸막이 등을 이용하여 비인가자 접근을 차단하여야 합니다.

■ 개인정보처리시스템에 대한 물리적 접근 통제 현황 등 증적자료를 위험도 분석 보고서에 첨부합니다.

22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용시 관리자 승인 후 사용하고 있습니까?

취 지

■ 2011년 N금융회사 전산망 마비 사태의 원인 중 하나는 노트북을 통한 보조기억매체(USB) 접속입니다. 방화벽, 침입탐지 등 네트워크 접근제한 솔루션을 운용한다 하더라도 DB서버 등에 보조기억매체 직접 접근으로 해킹프로그램 구동이 가능할 수 있고, 내부직원에 의한 개인정보의 직접 유출 가능성도 배제할 수 없습니다.₩

해 설

정 의

■ **보조기억매체란?**

- USB메모리, 외장형 하드디스크, CD, DVD, 디스켓 등 자료를 저장할 수 있는 일체의 것으로 개인정보처리시스템과 분리 할 수 있는 기억장치

■ DB서버나 DB접속 어플리케이션 서버에 직접 보조기억매체 삽입을 차단하고 불가피하게 업무목적으로 쓸 경우 관리자 허가를 받는 절차를 거쳐야 합니다.

■ 관리자는 보조기억매체의 사용을 통제하여야 하며, 최신 백신으로 악성코드 감염 여부를 확인하는 등 보안조치를 확인 후 사용을 허가하고 관리자 승인 내역을 전자적인 매체 또는 수기문서 대장에 기록하여야 합니다.

■ 보조기억매체 이용관리 현황 등 증적자료를 위험도 분석 보고서에 첨부합니다.

23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?

취 지

■ 보안패치는 운영체제나 응용프로그램에 내재된 보안 취약점을 보완하는 소프트웨어로 보안패치를 할 경우 취약점을 악용하는 악성코드 감염을 방지합니다.

해 설

■ 운영체제나 응용프로그램의 보안 취약점은 해커에 의한 공격 경로를 제공할 수 있으므로 운영체제 제조사 등에서 업데이트 공지가 있는 경우 최신 보안패치를 적용합니다.

■ '지체없이'란 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치에 대한 제조사 공지 후 적용하기 까지 소요되는 합리적인 상당시간을 의미합니다.

■ DB 접속 단말기의 운영체제 보안패치 현황 등 증적자료를 위험도 분석 결과보고서에 첨부합니다.

24. 하드디스크(HDD)등 DB 저장매체의 불용처리시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?

취 지

■ 저장매체의 폐기, 양여, 교체 등 불용처리로 저장매체에 저장된 개인정보는 모두 파기해서 외부에 노출되지 않도록 해야 하며, 복구될 수 없도록 완전하게 삭제해야 합니다. 암호화되지 않은 개인정보가 저장매체의 불용처리로 인해 외부에 반출되거나 복구될 경우 개인정보 유출 위험이 있습니다.

해 설

■ 파일을 삭제하거나 하드디스크를 포맷한 후 중고 PC로 매매하는 경우가 종종 있으나, 파일 삭제 또는 하드디스크 포맷만으로는 데이터 영역이 완전하게 삭제되지 않아 복구될 수 있습니다. 중고 PC에 개인정보가 남아 있을 경우 개인정보 오·남용의 위험성이 있으므로 이를 방지하기 위한 조치가 필요합니다.

■ 국가정보원이 저장매체 불용처리 지침을 마련한 바 있으며 개인정보 등이 저장된 하드디스크에 대한 삭제방법이 포함되어 있습니다.

저장매체	삭제 방법
플로피 디스크	완전파괴(소각, 파쇄, 용해)
광디스크(CD, DVD)	완전파괴(소각, 파쇄, 용해)
자기 테이프	완전파괴(소각, 파쇄, 용해) 또는 전용 소자(消磁)장비이용 삭제
반도체 메모리 (EEPROM 등)	완전파괴(소각, 파쇄, 용해) 또는 완전포맷 3회 수행
하드디스크	완전파괴(소각, 파쇄, 용해) 또는 전용 소자(消磁)장비이용 삭제 또는 완전포맷 3회 수행

※ 전용 소자장비 이용 삭제 : 소자장비는 반드시 저장매체의 자기력보다 큰 자기력 보유
완전포맷 3회 이상 수행 : 저장매체 전체를 '난수','0','1'를 각각 중복 저장하는 방식으로 삭제

■ DB저장매체 불용처리 절차 및 현황 등 관련 증적자료를 위험도 분석 결과보고서에 첨부합니다.

2-2-2 웹 기반

25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?

취 지

■ 개인정보가 내부망에 존재할 때 외부에서의 접근은 불가능 하지만 외부에 의해 해킹이 일어나는 경우는 대개 다른 시스템을 경유하여 일어나며 대표적으로는 외부에 오픈되어 있는 웹서버를 통하여 발생할 수 있습니다. 따라서, 웹서버를 경유한 해킹 방지를 위한 조치가 필요합니다.

해 설

■ 웹서버를 통한 외부자 해킹 방지를 위해 웹 취약점 진단을 정기적으로 실시하여 보완하거나 웹 방화벽을 통해 웹서버 자체에 대한 공격을 효과적으로 차단합니다.

■ 웹 취약점 진단

- 해커는 웹 서버 자체의 취약점을 직접 공격하거나 웹 어플리케이션의 취약점을 공격하여 개인정보를 유출합니다. DB에 외부로부터 접근할 수 있는 거의 유일한 통로이므로 웹 취약점에 대한 공격이 집중적으로 이루어져 대부분의 개인정보 유출사고의 경로가 됩니다.

- DB접근제어 솔루션을 적용하더라도 SQL Injection 등의 취약점 공격을 완벽히 막기는 어려우므로 웹 어플리케이션의 취약점 제거를 통해 이를 사전방지해야 합니다.

- 해킹기술이 발달하고 서비스 환경이 변화함에 따라 취약점은 계속 신규 발생하고 있으므로 년1회 이상 정기적인 웹 취약점 점검이 필요하며, 긴급한 취약점 발생 시에는 추가적인 취약점 점검을 통한 보완 조치가 필요합니다.

■ 웹 방화벽

- 웹서버를 통해 DB정보를 유출하고자 하는 SQL Injection, 웹서버 자체를 해킹하고자 하는 웹쉘 등의 공격을 효과적으로 방어하여 웹 해킹을 방지합니다.

■ 웹취약점 점검 현황 및 조치결과, 주기적 점검계획 등이 포함된 증적자료나 웹 방화벽 운영현황 등 웹서버 보호조치 현황을 위험도 분석 결과보고서에 첨부합니다.

26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까 ?

취 지

■ 보안패치는 운영체제나 응용프로그램에 내재된 보안 취약점을 보완하는 소프트웨어로 보안패치를 할 경우 취약점을 이용하는 악성코드 감염을 방지합니다.

해 설

■ 운영체제나 응용프로그램의 보안 취약점은 해커에 의한 공격 경로를 제공할 수 있으므로 운영체제 제조사 등에서 업데이트 공지가 있는 경우 최신 보안패치를 적용합니다.

■ '지체없이'란 현재 운영중인 응용프로그램과의 업무연속성, 시스템에 미칠 영향 등을 고려하여 적용하기 까지 소요되는 합리적인 상당시간을 의미합니다.

■ 웹서버의 보안패치 현황 등 증적자료를 위험도 분석 결과보고서에 첨부합니다.

3. 위험도 분석 결과보고서

■■■ 위험도 분석 결과보고서 ■■■

작성일	년 월 일	작성자	(소속)	(성명)
개인정보파일명				

(작성예제)

< 목 차 >

■ 「위험도 분석 결과보고서」에는 위험도분석 기준 작성에 대한 증적과 위험도 분석 점검에 따른 암호화 여부 등 위험도 분석 결과를 작성합니다.

■ 개인정보처리자는 위험도 분석 점검 내용에 대한 입증 책임이 있으며, 허위 작성을 방지하기 위하여 「위험도 분석 기준」의 점검 항목에 '예'로 체크했다면 그에 대한 증적을 명시하여야 합니다.

■ 「위험도 분석 점검 항목」에서 어느 하나의 점검항목이라도 '아니오'에 해당하는 경우, 암호화에 상응할만한 충분한 보호조치가 이루어지고 있다고 볼 수 없으므로 해당 개인정보파일에 대해 암호화 조치를 수행합니다.

■ 「위험도 분석 점검 항목」과 「위험도 분석 결과보고서」는 개인정보보호책임자 또는 해당 부서장의 결재를 득한 후 보관합니다.

■ 개인정보처리시스템 증설, 내·외부망 연계 등 기타 운영환경이 변경된 경우 위험도가 새롭게 발생될 수 있으므로 위험도 분석을 지속적으로 실시하여 개인정보의 안전한 관리가 가능하도록 조치합니다.