개인정보 암호화 조치 안내서

(Ver 1.0)

2012. 10.

행정안전부 KISA 한국인터넷진흥원

본 안내서는 “개인정보 보호법”에 따라 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적 보호조치 중 “암호화”에 대한 안내를 위해 마련하였습니다.

본 안내서는 개인정보처리자가 주민등록번호의 저장·전송시 필요한 암호화 수행방식과 사례 등을 소개하고 있으며 수록된 암호화 알고리즘 등은 2012년 10월 기준으로 작성되었습니다.

따라서 본 안내서 이용시 암호화 알고리즘에 대한 최신 정보를 확인하시기 바랍니다. 또한 개인정보처리시스템별 환경에 따라 사례 등의 적용방식이 달라질 수 있음을 알려드립니다.

목 차

목 차

Ⅰ 개 요

제1절 목적

❍ 개인정보 보호법에서는 개인정보에 대한 안전성 확보조치 의무를 규정하고 있으며 그중 하나로 암호화 조치를 수행토록 하고 있다.

❍ 본 안내서는 개인정보처리자가 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송·수신하거나 저장하는 경우 암호화 기준을 제시하고 적용방법 및 적용사례 등의 안내를 목적으로 한다.

<관련 근거>

☞ 「개인정보 보호법」제24조(고유식별정보의 처리제한) 제3항 및 동법 시행령 제21조(고유식별정보의 안전성 확보조치)

☞ 「개인정보 보호법」제29조(안전조치의무) 및 동법 시행령 제30조(개인정보의 안전성 확보조치)

☞ 「개인정보 보호법」시행령 제30조(개인정보의 안전성 확보조치) 제3항에 따른 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2011-제43호) 제7조

제2절 적용 대상

❍ 개인정보 보호법에 따라 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 저장·전송하는 개인정보처리자를 대상으로 한다.

제3절 용어 정의

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

- “개인정보취급자”는 개인정보처리자의 지휘, 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
- “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
- “개인정보처리시스템”이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
- “공공기관”이란 개인정보 보호법 제2조 및 동법시행령 제2조에 따른 국회, 법원, 헌법재판소, 중앙선관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체, 국가인권위원회, 공공기관의 운영에 관한 법률 제4조에 따른 공공기관, 지방공기업법에 따른 지방공사와 지방공단, 특별법에 따라 설립된 특수법인, 초·중등교육법, 고등교육법 및 그 밖의 다른 법률에 따라 설치된 각급 학교를 말한다.
- “내부망”이란 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
- “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 말한다.
- “보안서버”란 인터넷상에서 사용자 PC와 웹서버 사이에 송·수신되는 개인정보를 암호화하여 전송하는 서버를 말한다.
- “보조저장매체”라 함은 이동형 하드디스크(HDD), USB메모리, CD (Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.
- “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

❍ “소상공인”이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.

❍ “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

❍ “인증정보”란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.

❍ “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

❍ “정보통신망”이란 ’전기통신기본법’ 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체계를 말한다.

Ⅱ 암호화 종류 및 제도

제1절 암호화의 필요성

- 정보통신 기술 발전에 따라 개인정보의 저장·유통이 대량화, 광역화, 네트워크화 되고 있어 이렇게 저장·유통되는 개인정보는 다양한 위협에 쉽게 노출되고 있다.
- 공격자는 정보통신망을 통해 개인정보 송수신시 패킷 도청 소프트웨어를 사용하여 가로채거나 또는 개인정보가 저장된 서버의 취약점을 찾아 고유식별정보 등과 같은 중요한 개인정보를 해킹하게 된다. 이러한 위협으로부터 중요 정보를 보호하기 위해서 개인정보의 전송 및 저장시 암호화가 필요하다.
- 암호화란 일상적인 문자로 쓰인 평문을 암호키를 소유하지 않은 사람이 알아볼 수 없도록 기호 또는 다른 문자 등의 암호문으로 변환하는 방법으로 정보의 기밀성 및 무결성, 사용자 인증 등을 위해 광범위하게 이용하고 있다.
- 최근 사회 전 분야에 걸쳐 개인정보 유출사고의 지속적인 발생으로 인해 제정된 개인정보보호법에 개인정보에 대한 안전성을 확보하기 위한 조치의무를 규정하고 있으며 전송 또는 저장 정보의 암호화 조치는 선택이 아닌 반드시 수행해야 할 항목으로서 위치하고 있다.

제2절 암호화 종류 및 특징

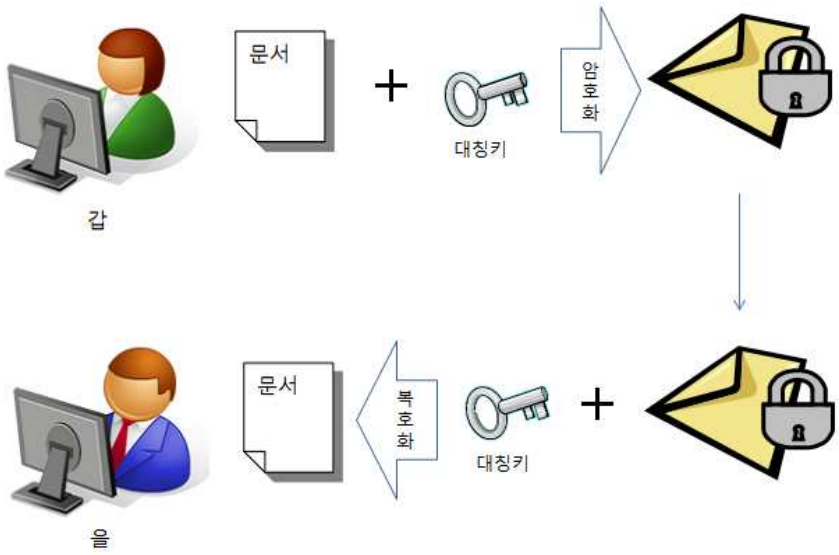
2.1 대칭키 암호화

- 대칭키 암호화 방식은 전송하고자 하는 평문을 암호화하고 복호화하는데 동일한 키를 사용하는 방식이다.
- 대칭키 암호화 방식은 공개키 암호화 방식에 비해 빠른 처리속도를 제공하고, 암호키의 길이가 공개키 암호화 방식보다 상대적으로 작아서 일반적인 정보의 기밀성을 보장하기 위한 용도로 사용되고 있다.

❍ 반면에 정보 교환 당사자 간에 동일한 키를 공유해야 하므로 여러 사람과의 정보 교환 시 많은 키를 유지 및 관리해야 하는 어려움이 있다.

❍ 대표적인 대칭키 암호 알고리즘은 국내의 SEED, ARIA, 미국의 DES, Triple-DES, AES, 유럽의 IDEA, 일본의 FEAL, MISTY 등이 있다.

❍ 대칭키 암호화 방식의 기본 개념은 <그림 1>과 같다.



<그림 1 > 대칭키 암호화 방식

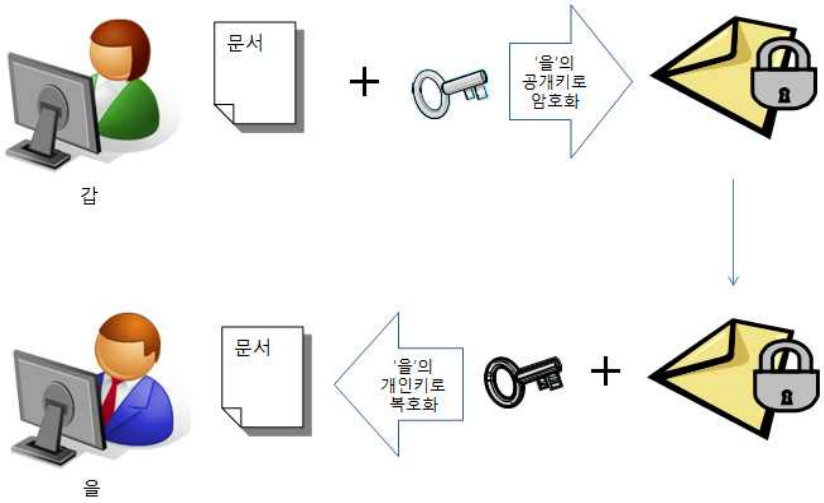
2.2 공개키 암호화

❍ 공개키 암호화 방식은 공개키와 개인키의 키 쌍이 존재하여 평문을 암·복호화하는데 서로 다른 키를 사용하는 방식으로 비대칭키 암호화 방식이라고도 불린다,

❍ 공개키 암호화 방식은 데이터 암호화 속도가 대칭키 암호화 방식에 비해 느리기 때문에 일반적으로 대칭키 암호화 방식의 키 분배나 전자서명 또는 카드번호와 같은 작은 크기의 데이터 암호화에 많이 사용되고 있다.

❍ 대표적인 공개키 암호 알고리즘으로는 국내에는 KCDSA가 있으며 국외에서는 RSA, ElGamal, ECC 등이 있다.

❍ 공개키 암호화 방식의 기본 개념은 <그림 2>와 같다.



<그림 2> 공개키 암호화 방식

2.3 일방향(해쉬함수) 암호화

❍ 일방향 암호화 방식은 해쉬함수를 이용하여 암호화된 값을 생성하며 복호화 되지 않는 방식이다.

❍ 해쉬함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해쉬값만으로 입력 메시지를 유추할 수 없어 전자서명 체계와 함께 데이터의 무결성을 위해 사용된다. 비밀번호와 같이 복호화가 필요 없지만 입력 값의 정확성 검증이 필요한 경우에 사용하고 있다.

❍ 대표적인 해쉬함수로는 SHA-2(SHA-224/256/384/512), RIPEMD-160 등과 국내에서 개발한 HAS-160이 있다.

제3절 안전한 암호 알고리즘

❍ 개인정보의 안전성 확보조치 기준 제7조제6항의 '안전한 암호알고리즘(이하 '암호알고리즘'이라 한다)'이란 국내외 전문기관에서 권고하는 알고리즘을 의미한다.

❍ 국내외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)의 권고를 중심으로 구성하고 있으며 이에 따른 암호 알고리즘은 [표 1]과 같다.

[표 1] 안전한 암호 알고리즘(예시)

구분	알고리즘 명칭
대칭키 암호 알고리즘	SEED ARIA-128/192/256 AES-128/192/256 Blowfish Camelia-128/192/256 MISTY1 KASUMI 등
공개키 암호 알고리즘	RSA KCDSA(전자서명용) RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/256/384/512 Whirlpool 등

※ 공공기관은 "[붙임 1] 국가정보원(IT보안인증사무국) 검증대상 암호알고리즘 목록"을 참고

- 본 안내서에서 권고하는 암호 알고리즘 등은 2012년 10월 기준으로 작성됨에 따라 국내외 암호전문기관의 최신 정보를 반드시 확인하도록 한다.

3.1 SEED

❍ SEED는 순수 국내기술로 개발한 대칭키 암호 알고리즘으로 128/256 비트 키를 지원하며, 128 비트 지원의 경우 1999년 정보통신단체표준(TTA)으로 제정되었으며, 2005년에는 국제 표준화 기구인 ISO/IEC와 IETF의 블록 암호 알고리즘 표준으로 제정되었다.

3.2 ARIA-128/192/256

❍ ARIA는 대칭키 방식의 국가 암호화 알고리즘으로 128 비트 블록 단위로 데이터의 암호화, 복호화를 수행하는 블록 암호 알고리즘이다. 128/192/256 비트 키를 지원하며 2004년에 한국산업규격 KS 표준으로 제정되었다.

3.3 SHA-224/256/384/512

❍ SHA는 해쉬함수로서 1993년 미국 표준기술연구소(NIST)에서 해쉬함수의 표준으로 개발한 SHA-1에 보안 취약점의 존재 가능성이 제기됨에 따라 SHA-2라는 명칭으로 해쉬값의 크기가 224/256/384/512 비트를 가지는 SHA-224/256/384/512의 해쉬함수가 표준화 되었다.

3.4 AES-128/192/256

❍ AES는 미국 표준기술연구소(NIST)에서 연방 정보처리 표준으로 발표한 대칭키 암호 알고리즘으로 128 비트의 블록크기를 가지며 키 길이는 128/192/256 비트를 가진다. 키 길이가 가변적이고 라운드 수도 블록 크기에 따라 가변적인 알고리즘으로 안전성과 성능의 요구에 따라 유연하게 사용이 가능하다.

3.5 Blowfish

❍ 1993년 개발한 대칭키 암호 알고리즘으로 가변적인 키 길이(32~448 비트)를 가지며, 구현이 간단하고 알고리즘의 안전성을 분석하기 쉬우며, 키의 크기가 가변적이므로 안전성과 성능의 요구에 따라 유연하게 사용이 가능하다.

3.6 RSA

❍ RSA는 1983년에 미국 매사추세츠 공과대학교(MIT)에서 개발한 공개키 암호 알고리즘의 하나로 소인수분해의 어려움에 안전성의 기반을 두고 있으며, 대칭키 암호 알고리즘과 달리 메시지 암호화 등에 사용할 수 있도록 상대방에게 공개하는 공개키와 공개키로 암호화된 메시지를 복호화하는데 사용되는 비밀키를 사용한다. RSA 알고리즘을 활용한 암호시스템은 대칭키의 안전한 분배 및 관리문제를 해결하기 위해 널리 이용되며, 메시지 암·복호화, 전자서명 등에 사용된다.

3.7 Hash_DRBG

❍ Hash_DRBG는 해쉬함수를 이용하여 의사난수를 생성하는 난수발생기이다. 난수는 암호학적으로 대칭키 암호 알고리즘의 비밀키, 스트림암호 알고리즘의 초기화벡터, 공개키 암호 알고리즘 RSA의 큰 소수 등을 생성할 때 사용되는 것으로 난수를 생성하는 과정의 안전성에 결함이 있다면 이는 암호 알고리즘 자체의 안전성에 영향을 미치게 된다. Hash_DRBG는 이러한 난수를 해쉬함수를 이용해 안전하게 생성하는 난수발생기이며 HAS-160, SHA-2 등의 해쉬함수를 사용할 수 있다.

제4절 암호화 관련 제도

4.1 개인정보 보호법

4.1.1 적용 대상

❍ 공공기관, 법인, 단체 및 개인을 포함한 모든 개인정보처리자를 적용 대상으로 한다.

4.1.2 암호화 관련 주요 내용

❍ 개인정보 보호법 제24조 제3항

> **제24조(고유식별정보의 처리 제한)**
> ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 **대통령령**으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

❍ 개인정보 보호법 제29조

> **제29조(안전조치의무)**
> 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 **대통령령**으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

❍ 개인정보 보호법 시행령 제30조 제1항 제3호 및 제3항

> **제30조(개인정보의 안전성 확보 조치)**
> ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
> 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
> ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다.

❍ 개인정보 보호법 시행령 제30조 제3항에 따른 '개인정보의 안전성 확보조치 기준 제7조'(행정안전부고시 제2011-제43호)

※ 세부 설명은 '[붙임 2] 개인정보 보호법 암호화 관련 세부 내용' 참조

• 개인정보 위험도 분석기준 및 해설서(행정안전부 공고 제2012-112)는 www.privacy.go.kr에서 다운로드 받을 수 있다.

4.2 전자정부법

4.2.1 적용 대상

❍ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 소속기관, 지방자치단체 및 공공기관을 대상으로 한다.

4.2.2 암호화 관련 주요 내용

❍ 전자정부법 제56조

제56조(정보통신망 등의 보안대책 수립·시행)

① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다.

② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다.

③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.

④ 제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다.

❍ 전자정부법시행령 제69조, 제70조

제69조(전자문서의 보관·유통 관련 보안조치)

① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.

1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용
2. 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행

② 행정기관의 장이 제1항의 보안조치를 이행하는 경우에는 미리 국가정보원장에게 보안성 검토를 요청하여야 한다.

③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치에 관하여 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.

제70조(보안조치 이행 여부의 확인)

① 국가정보원장은 법 제56조제3항에 따라 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부를 확인하는 경우 점검항목·절차·시기 등에 관하여 해당 행정기관의 장에게 미리 통보하여야 한다.

② 국가정보원장은 이행 여부의 확인 결과 신속한 시정이 필요하다고 판단하는 경우에는 행정기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 요청을 받은 행정기관의 장은 특별한 사유가 없으면 이에 따라야 한다.

③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부 확인에 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.

4.3 정보통신망 이용촉진 및 정보보호 등에 관한 법률

4.3.1 적용 대상

❍ 정보통신서비스 제공자(기간통신사업자, 별정통신사업자, 부가통신사업자), 방송사업자 등이 적용 대상에 해당한다.

4.3.2 암호화 관련 주요 내용

❍ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조

제28조(개인정보의 보호조치)

① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치

❍ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조 제4항 및 6항

제15조(개인정보의 보호조치)

④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장
2. 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안조치

⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

❍ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조 제6항에 따른 '개인정보의 기술적·관리적 보호조치 기준 제6조' (방송통신위원회 고시 제2012-50호)

제6조(개인정보의 암호화)

① 정보통신서비스 제공자등은 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

4.4 전자금융거래법, 전자금융감독규정

4.4.1 적용 대상

❍ 은행, 금융투자업자, 증권금융회사, 종합금융회사, 명의개서대행회사, 보험회사, 상호저축은행 및 그 중앙회, 신용협동조합 및 그 중앙회, 여신전문금융회사, 농협은행 및 조합, 수산업 협동조합 및 그 중앙회의 신용사업부문, 산림조합 및 그 중앙회의 신용사업부문, 체신관서, 새마을금고 및 새마을금고연합회, 한국거래소, 한국예탁결제원, 금융지주회사 및 전산자회사, 전자금융업자 기타 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자를 적용 대상으로 한다.

4.4.2 암호화 관련 주요 내용

❍ 전자금융거래법 제21조

제21조(안전성의 확보의무)

① 금융기관·전자금융업자 및 전자금융보조업자(이하 "금융기관등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

② 금융기관등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준을 준수하여야 한다. <개정 2008.2.29>

③ 금융위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 「전자서명법」 제2조제8호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다. <개정 2008.2.29>

❍ 전자금융감독규정 제15조, 제17조, 제31조, 제32조, 제33조, 제34조, 제60조

제15조(해킹 등 방지대책)

① 금융기관 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 단말기에서 제1호의 규정에 따른 정보보호시스템을 우회한 인터넷 등 외부통신망(무선통신망을 포함한다) 접속 금지

② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 정보보호시스템에 사용하는 정보보호제품은 국가기관의 평가·인증을 받은 장비를 사용할 것
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것
4. 정보보호시스템의 원격관리를 금지하고 주기적으로 작동 상태를 점검할 것
5. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것

③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.

④ 금융기관 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.

⑤ 금융기관 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 사고에 대비하여 정보처리시스템 및 정보통신망에 대해서 매년 취약점을 분석·평가하고 그 이행계획을

수립·시행하여야 한다.

⑥ 금융기관 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.

1. 무선통신망 이용 업무는 최소한으로 국한하고 소관 부서장의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 지정된 업무 용도와 사용 지역(zone) 이외 무선통신망 접속을 차단하기 위한 차단 시스템 구축 및 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

제17조(홈페이지 등 공개용 웹서버 관리대책)

① 금융기관 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것

2. 공개용 웹서버에 접근할 수 있는 사용자계정을 업무관련자만 접속할 수 있도록 제한하고 불필요한 계정 또는 서비스번호(port)는 삭제할 것(다만, 사용자계정은 아이디 및 비밀번호 이외에 제37조에 따른 공인인증서 등을 추가 인증수단으로 반드시 적용하여야 한다)
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

② 금융기관 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지
3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 금융기관 또는 전자금융업자는 홈페이지 등 공개용 웹서버에 대해 6개월마다 취약점을 분석·평가하고 그 이행계획을 수립·시행하여야 한다.

④ 금융기관 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 다음 각 호에 대하여 적절하게 대응 조치하여야 한다.

1. 악의적인 명령어 주입 공격(SQL injection)
2. 업로드 취약점

3. 취약한 세션 관리(cookie injection)
4. 악의적인 명령 실행(XSS)
5. 버퍼 오버플로우(buffer overflow)
6. 부적절한 파라미터(parameter)
7. 접근통제 취약점
8. 서버설정과 관련한 부적절한 환경설정 취약점

⑤ 금융기관 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

제31조(암호프로그램 및 키 관리 통제)

① 금융기관 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다.

② 금융기관 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.

제32조(내부사용자 비밀번호 관리)

금융기관 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   가. 제12조제3호에 따라 비밀번호 부여 및 변경
   나. 비밀번호 보관 시 암호화
   다. 시스템마다 관리자 비밀번호를 다르게 부여
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

제33조(이용자 비밀번호 관리)

① 금융기관 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.

② 금융기관 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시

해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)

4. 금융기관이 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

제34조(전자금융거래 시 준수사항)

① 금융기관 또는 전자금융업자는 다음의 경우를 제외하고는 전자자금이체 시 보안카드를 포함한 일회용 비밀번호를 적용하여야 한다.

1. 자동화기기(CD/ATM)를 이용한 자금이체의 경우
2. 제휴 금융기관에서 실명 확인 후 개설된 증권계좌와 연계된 본인명의의 실명확인 계좌로 이체하는 경우
3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자를 방문하여 등록한 실명 확인된 본인 명의 계좌로 이체하는 경우
4. 신용카드 대출서비스를 실명 확인된 본인명의 계좌로 이체하는 경우
5. 보험회사의 보험금, 대출금 등을 실명 확인된 본인명의의 보험료납입 계좌로 이체하는 경우
6. 법인이 금융기관과 연결된 전용회선을 이용하여 전자자금이체를 하는 경우
7. 등록금, 원서접수비 등 본인확인이 가능하고 입금계좌가 지정되어 있는 경우
8. 그 밖에 금융감독원장이 필요하다고 인정하는 경우

② 금융기관 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 보안성심의를 받은 경우에는 그러하지 아니하다)
2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
3. 해킹 등 침해행위로부터 전자금융거래를 보호하기 위해 이용자의 전자적 장치에 보안프로그램 설치 등 보안대책을 적용할 것(다만, 고객의 책임으로 본인이 동의하는 경우에는 보안프로그램을 해제할 수 있다)
4. 전자금융거래에 사용되는 일회용 비밀번호(OTP를 포함한다. 이하 이 조에서 같다) 등의 접근매체를 발급받기 위해서는 반드시 본인 실명증표를 확인한 후 교부할 것
5. 전자금융거래수단이 되는 매체와 일회용 비밀번호 등 거래인증수단이 되는 매체를 분리하여 사용할 것

6. 비밀번호 개수가 한정된 일회용 비밀번호 사용 시에 비밀번호 입력 오류가 발생하거나 일회용 비밀번호를 입력하지 않고 비정상적으로 거래를 종료하면, 다음 거래 시 동일한 비밀번호를 요구할 것
7. 금융기관 또는 전자금융업자는 전자금융거래에서 이용자에 게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

제60조(외부주문등에 대한 기준)

① 금융기관 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 정보처리시스템 설치장소에 대한 통제
2. 금융기관과 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지

Ⅲ 개인정보 암호화 방식

제1절 전송시 암호화

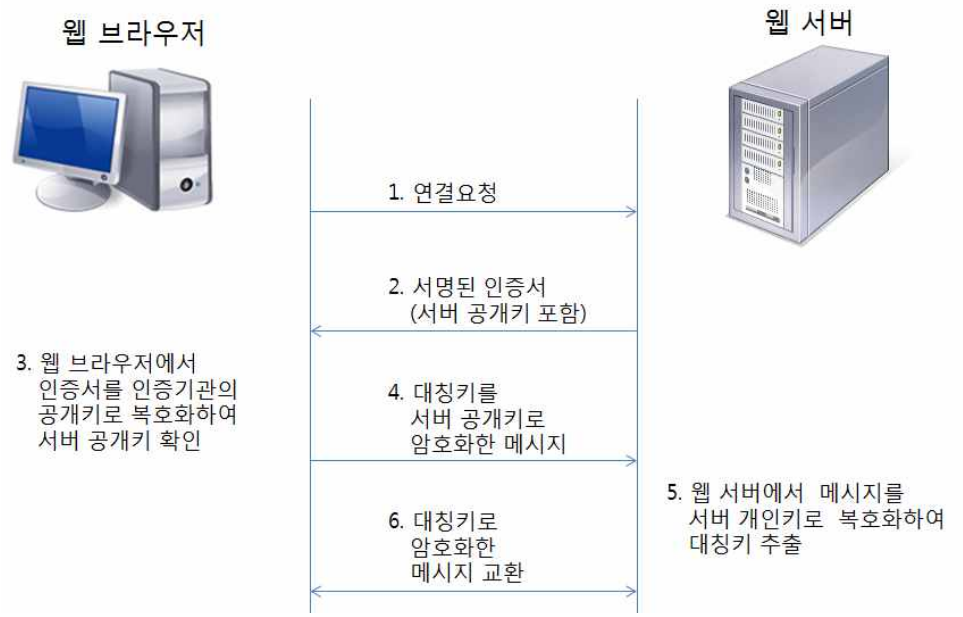
1.1 웹서버와 클라이언트 간 암호화

- 웹서버와 클라이언트 간 개인정보 전송시 암호화를 위하여 공인인증기관이 발급한 서버 인증서를 설치한 보안서버를 사용하는 방식으로 웹브라우저에 기본적으로 내장된 SSL/TLS 프로토콜로 접속하는 SSL 방식과 웹브라우저에 보안 프로그램을 설치하여 접속하는 응용프로그램 방식으로 구분할 수 있다.
- SSL 방식은 웹페이지 전체를 암호화(웹페이지내 이미지 포함)하며 응용프로그램 방식은 특정 데이터만을 선택적으로 암호화할 수 있지만, 보안서버와 웹브라우저에 부가적인 프로그램을 설치해야 한다.
- 공공기관에서는 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용해야 한다.

1.1.1 SSL 방식

- SSL 방식은 전송 계층(Transport Layer)을 기반으로 한 응용 계층(Application Layer)에서 암호화를 수행한다. 암호키교환은 비대칭키 암호 알고리즘을 이용하고, 기밀성을 위한 암호화는 대칭키 암호 알고리즘을 이용하며 메시지의 무결성은 메시지 인증 코드(해쉬함수)를 이용하여 보장한다.
- 인터넷 쇼핑이나 인터넷 뱅킹 시 계좌정보 및 주민등록번호 등과 같은 중요한 정보를 입력할 때, 거래당사자의 신원 및 거래내용의 위·변조 여부를 확인하고 중요 정보가 제3자에게 유출되는 것을 막기 위해 SSL/TLS와 같은 통신 암호기술을 이용할 수 있다.
- <그림 3>은 인증기관으로부터 인증서를 발급받은 웹서버와 사용자의 웹브라우저 간 SSL/TLS를 이용한 보안 통신의 개념을 간단하게 소개하고 있다. 사용자가 웹서버에 처음 접속하면 인증서 및 통신 암호화에 이용할 암호키를 생성하기 위한 정보를 공유하고, 이후 공유된 정보를 통해 생성된 암호키를 이용하여 데이터를 암호화하여 전송한다.

❍ SSL/TLS 통신을 하는 경우에는 로그인 페이지 등 보안이 필요한 웹페이지에 접속하면 웹브라우저 하단 상태 표시줄에 자물쇠 모양의 표시를 확인할 수 있다.



<그림 3> 웹서버와 웹브라우저 간의 SSL/TLS 통신 구조

1.1.2 응용프로그램 방식

❍ 응용프로그램 방식은 별도의 모듈을 서버와 클라이언트에 설치해야 하며 필요한 데이터만 암호화하여 전달할 수 있다. 이를 위해 웹서버 프로그램에 대한 수정작업이 필요하며, 응용프로그램 방식을 제공하는 솔루션에 따라 수정작업의 범위가 달라질 수 있다.

❍ 보안서버를 구현한 웹서버에 사용자가 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되고 이를 통해 개인정보를 암호화하여 통신이 이루어진다. 웹브라우저의 확장기능인 플러그인 형태로 구현되며 웹사이트 접속 시 초기화면이나 로그인 후 윈도우 화면 오른쪽 하단 작업표시줄 알림영역을 확인하여 프로그램이 실행되고 있음을 알 수 있다.

1.2 개인정보처리시스템 간 암호화

❍ 개인정보처리시스템 간에 개인정보를 전송할 때 암호화를 지원하기 위하여 공중망을 이용한 VPN(가상사설망)을 구축할 수 있다.

❍ VPN은 기반이 되는 보안 프로토콜의 종류에 따라 IPsec VPN 방식, SSL VPN 방식, SSH VPN 방식 등으로 구분할 수 있으며, 개인정보처리시스템 간의 통신에서 사용할 수 있는 VPN 전송 방식의 특징을 간단히 비교하면 [표 2]와 같다.

[표 2] 개인정보처리시스템 간 전송시 암호화 방식 비교

방식	VPN 서버부하	NAT 통과
IPsec VPN	낮음	어려움
SSL VPN	다소 높음	쉬움
SSH VPN	다소 높음	쉬움

※ NAT(Network Address Translation) : 사설 IP 주소를 공인 IP 주소로 바꿔주는데 사용하는 통신망의 주소변환기

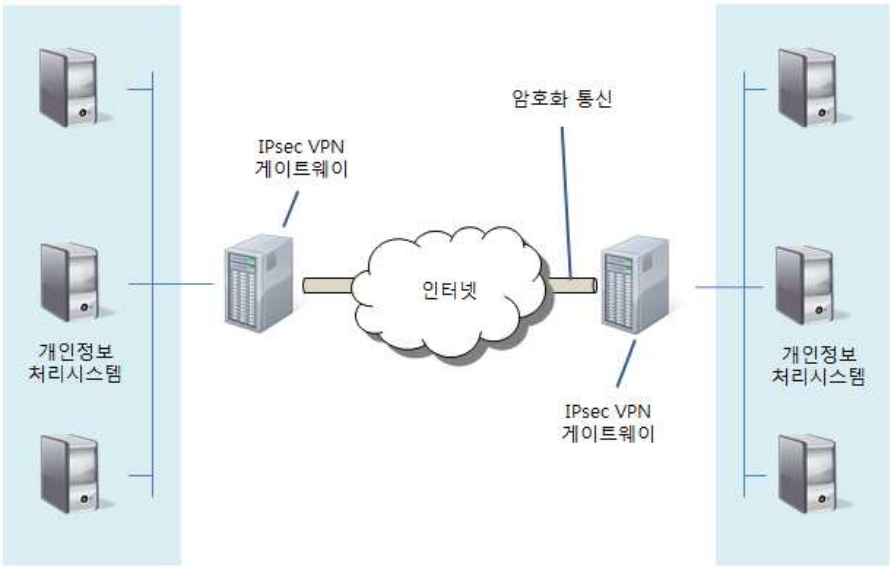
❍ VPN은 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하고 수신측에서 이를 복호화 하는 방식으로 송·수신 정보에 대한 기밀성 및 무결성을 보장하며, 그 외에도 데이터 출처 인증, 재전송 방지, 접근제어 등 다양한 보안 기능을 제공한다.

1.2.1 IPsec VPN 방식

❍ IPsec VPN 방식은 응용프로그램을 수정할 필요가 없으나 IPsec 패킷의 IP 주소를 변경해야 하는 NAT와 같이 사용하기 어려운 점이 있다. 사용자 인증이 필요 없으므로 VPN 장비 간 서로 인증이 된 경우, 사용자는 다른 인증절차를 거치지 않아도 된다.

❍ IPsec VPN 방식의 구조는 게이트웨이 대 게이트웨이, 호스트 대 게이트웨이, 호스트 대 호스트로 구분할 수 있다. 게이트웨이 대 게이트웨이는 네트워크 간의 암호화 통신, 호스트 대 게이트웨이는 개인정보처리시스템과 네트워크 간의 암호화 통신, 호스트 대 호스트는 개인정보처리시스템 간의 암호화 통신을 설정할 수 있다.

❍ <그림 4>는 게이트웨이 대 게이트웨이 IPsec VPN 방식을 이용하여 인터넷을 통과하는 암호화 통신을 보여준다.

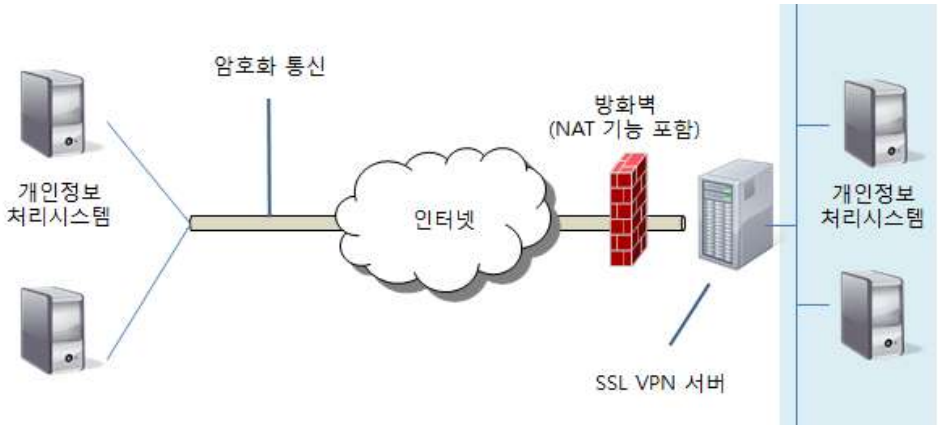


<그림 4> IPsec VPN 방식(게이트웨이 대 게이트웨이)의 개념도

1.2.2 SSL VPN 방식

❍ SSL VPN 방식은 응용프로그램 수준에서 SSL/TLS을 구현하는 것이 일반적이며 NAT를 사용할 수 있다. SSL/TLS는 메모리 소비가 많으므로 동시 접속이 많은 대용량 처리에서 성능 저하가 발생할 수 있다. 하지만 개별 사용자 인증이 필요한 경우 SSL VPN 방식이 좋은 선택이 될 수 있다.

❍ <그림 5>는 SSL VPN 방식에서 SSL VPN 서버를 거친 개인정보처리시스템 간의 암호화 통신을 보여준다. 이러한 구조는 방화벽 외부에 위치한 개인정보처리시스템과 SSL VPN 서버가 설치된 LAN에 위치한 개인정보처리시스템 간의 통신에 이용이 가능하다.

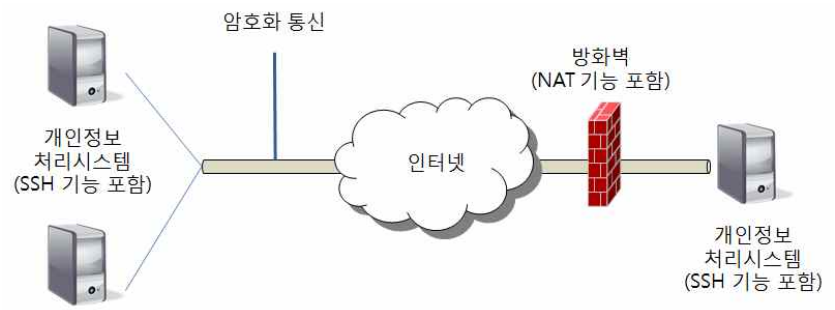


<그림 5> SSL VPN 방식의 개념도

1.2.3 SSH VPN 방식

❍ SSH VPN 방식은 응용계층의 VPN 기술로서 원격 단말기에서 접속하는 경우에 주로 이용되며 SSH를 이용한 파일 전송 및 파일 복사 프로토콜(예: SFTP, SCP)을 이용할 수 있다. 오픈소스 SSH의 일종인 OpenSSH의 경우 프락시 방식의 VPN 서버로 구성할 수도 있다.

❍ <그림 6>은 SSH VPN 방식에서 개인정보처리시스템 간의 암호화 통신을 보여준다. 각 개인정보처리시스템에 설치된 SSH 기능을 사용하여 VPN을 구성할 수 있다.



<그림 6> SSH VPN 방식의 개념도

TIP
- 개인정보처리시스템 간 전송시 공중망과 분리된 전용선을 사용하면 암호화에 상응하는 보안성을 제공할 수 있다.

1.3 개인정보취급자 간 암호화

❍ 개인정보취급자 간에 개인정보를 전송할 때 주로 이메일을 이용하게 된다. 이메일은 네트워크를 통해 전송되는 과정에서 공격자에 의해 유출되거나 위조될 가능성이 있다. 이러한 위협으로부터 이메일로 전송되는 메시지를 보호하기 위해서 PGP 또는 S/MIME을 이용하는 이메일 암호화 방식과 암호화된 파일을 이메일에 첨부하여 전송하는 이메일 첨부문서 암호화 방식이 있다.

• 개인정보취급자 간에 이메일을 사용하지 않고 직접 파일을 전송하고자 하는 경우는 개인정보처리시스템 간 전송시 암호화 방식의 VPN 기능을 적용할 수 있다.

❍ 개인정보취급자 간에 이메일을 전송할 때 사용되는 암호화 방식의 특징은 [표 3]과 같다.

[표 3] 개인정보취급자 간 전송시 암호화 방식 비교

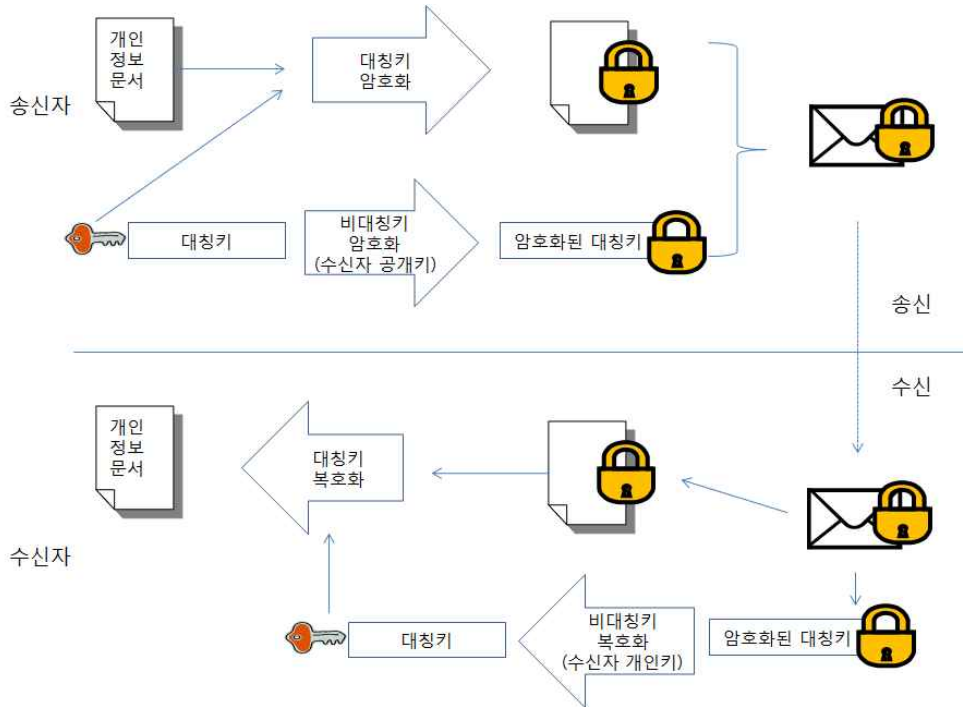
방식		공인인증서 필요 여부	표준형식
이메일 암호화	PGP	필요하지 않음	PGP 자체정의
	S/MIME	필요함	X.509, PKCS#7
이메일 첨부문서 암호화		필요하지 않음	없음

❍ S/MIME은 공개키를 포함한 공인인증서를 발급받고 등록해야 하는 번거로움이 있다. 이에 비해 PGP의 경우 개인 간의 신뢰를 바탕으로 공개키를 등록하거나 안전한 채널로 미리 확보하는 방법을 사용할 수 있다.

1.3.1 이메일 암호화 방식

❍ 이메일 암호화 방식은 송·수신되는 이메일의 내용을 암호화함으로써 메일 내 중요 개인정보의 유출을 방지하는 것이며, 대표적인 이메일 보안 프로토콜로는 PGP와 S/MIME이 있다. <그림 7>은 이메일 암호화 방식의 처리 과정을

보여준다.



<그림 7> 이메일 암호화 방식의 개념도

❍ PGP는 다양한 응용프로그램에 적용하여 문서, 이메일, 파일, 파일시스템, 디스크 등을 암호화할 수 있다.

❍ S/MIME은 인증, 메시지 무결성, 부인방지, 메시지 암호화 등에 사용되며 대부분의 이메일 클라이언트에서 기본적으로 지원한다. S/MIME을 사용하기 위해서는 공인인증기관이 발행한 공인인증서가 있어야 한다.

1.3.2 이메일 첨부문서 암호화 방식

❍ 업무용 컴퓨터에서 주로 사용하는 문서 도구(예: 흔글, MS 워드 등)의 자체 암호화 방식, 암호 유틸리티를 이용한 암호화 방식 등을 통해 암호화한 파일을 이메일의 첨부문서로 송·수신할 수 있다.[1)]

❍ 이메일을 송·수신할 개인정보취급자 간에는 암호키(또는 비밀번호)를 안전하게 공유하여야 한다.

1) 파일 암호화 방식은 'III장 2.2 업무용 컴퓨터 암호화'를 참고

제2절 저장시 암호화

2.1 개인정보처리시스템 암호화

2.1.1 개요

❍ 개인정보를 처리하고 관리하는 개인정보처리시스템은 DB에 저장된 개인정보를 암호화하여 저장함으로써 개인정보의 변경, 파괴 및 유출을 방지해야 한다.

❍ 개인정보처리시스템의 DB를 암호화할 수 있는 방식은 암·복호화 모듈의 위치와 암·복호화 모듈의 요청 위치의 조합에 따라 [표 4]와 같이 구분할 수 있다.

[표 4] 개인정보처리시스템 암호화 방식의 구분

방식	암·복호화 모듈 위치	암·복호화 요청 위치	주요 내용
응용 프로그램 자체 암호화	어플리케이션 서버	응용 프로그램	• 암·복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고, 응용프로그램에서 해당 암·복호화 모듈을 호출하는 방식 • DB 서버에 영향을 주지 않아 DB 서버의 성능 저하가 적은 편이지만 구축시 응용프로그램 전체 또는 일부 수정 필요 • 기존 API 방식과 유사
DB 서버 암호화	DB 서버	DB 서버	• 암·복호화 모듈이 DB 서버에 설치되고 DB 서버에서 암·복호화 모듈을 호출하는 방식 • 구축 시 응용프로그램의 수정을 최소화할 수 있으나 DB 서버에 부하가 발생하며 DB 스키마의 추가 필요 • 기존 Plug-In 방식과 유사
DBMS 자체 암호화	DB 서버	DBMS 엔진	• DB 서버의 DBMS 커널이 자체적으로 암·복호화 기능을 수행하는 방식 • 구축 시 응용프로그램 수정이 거의 없으나, DBMS에서 DB 스키마의 지정 필요 • 기존 커널 방식(TDE)과 유사

방식	암·복호화 모듈 위치	암·복호화 요청 위치	주요 내용
DBMS 암호화 기능 호출	DB 서버	응용 프로그램	• 응용프로그램에서 DB 서버의 DBMS 커널이 제공하는 암·복호화 API를 호출하는 방식 • 구축 시 암·복호화 API를 사용하는 응용프로그램의 수정이 필요 • 기존 커널 방식(DBMS 함수 호출)과 유사
운영체제 암호화	파일 서버	운영체제 (OS)	• OS에서 발생하는 물리적인 입출력(I/O)을 이용한 암·복호화 방식으로 DBMS의 데이터파일 암호화 • DB 서버의 성능 저하가 상대적으로 적으나 OS, DBMS, 저장장치와의 호환성 검토 필요 • 기존 DB 파일암호화 방식과 유사

• 각 방식의 단점을 보완하기 위하여 두 가지 이상의 방식을 혼합하여 구현하기도 한다. 이 경우, 구축 시 많은 비용이 소요되지만 어플리케이션 서버 및 DB 서버의 성능과 보안성을 높일 수 있다.

❍ 개인정보처리시스템 암호화 방식마다 성능에 미치는 영향이 다르므로 구축 환경에 따라 암호화 방식의 특성, 장단점 및 제약사항 등을 고려하여 DB 암호화 방식을 선택해야 한다. [표 5]는 개인정보처리시스템 암호화 방식의 선택 시 고려해야 할 사항이다.

[표 5] 개인정보처리시스템 암호화 방식 선택 시 고려사항

분 류	항 목
일반적 고려사항	구현 용이성, 구축 비용, 기술지원 및 유지보수 여부
	암호화 성능 및 안전성
	공공기관의 경우, 국가정보원 인증 또는 검증 여부
기술적 고려사항	암·복호화 위치(어플리케이션 서버, DB 서버, 파일서버 등)
	색인검색 가능 유무, 배치처리 가능 여부

- 성능이 매우 중요한 요소가 되는 환경에서 DB 서버 암호화 방식을 고려하는 경우에는 반드시 벤치마킹 테스트(BMT) 등을 수행하여, 최적의 솔루션을 선택하는 것이 바람직하다.

❍ 공공기관에서는 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용해야 한다.[2)]

❍ 암·복호화 모듈의 위치와 암·복호화 요청 위치에 따라 어플리케이션 서버 또는 DB 서버의 성능에 영향을 미칠 수 있다. 예를 들어, DB 서버 암호화 방식은 암·복호화 시 DB 서버의 자원을 추가적으로 사용하므로 대량의 트랜잭션 작업에서 DB 서버의 성능 저하가 발생할 수 있다.

❍ 현재 운영 중이거나 향후 개발 예정인 개인정보처리시스템의 목적 및 환경에 맞게 쉽게 구현이 가능한 암호화 방식을 선택해야 한다. 응용프로그램 및 DB 스키마 수정 등을 최소화하고 개발 환경에 맞게 성능을 최대화할 수 있도록 해야 한다.

❍ DB 암호화의 안전성을 확보하기 위해서는 안전한 암호키의 관리가 필요하다. 암호화된 개인정보가 유출되더라도 복호화 할 수 없도록 암호키에 대한 추가적인 보안과 제한된 관리자만 허용하도록 하는 기술의 적용을 권고한다.

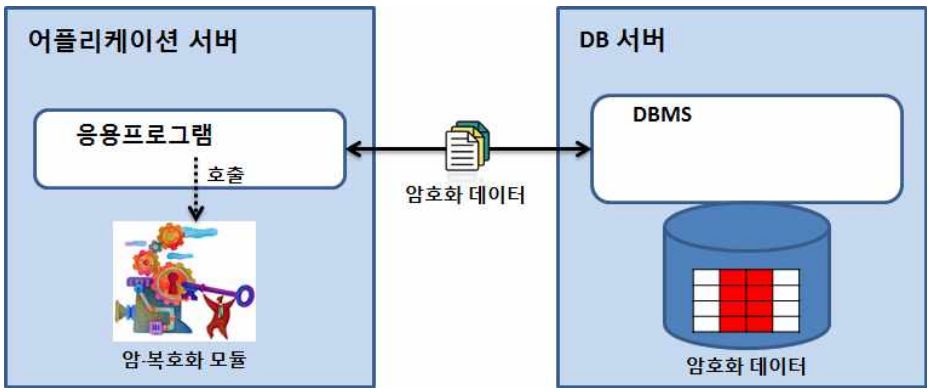
2) IT보안인증사무국(http://service1.nis.go.kr)의 검증필 암호 모듈 또는 제품 확인이 가능함

2.1.2 응용프로그램 자체 암호화 방식

❍ 응용프로그램 자체 암호화 방식은 <그림 8>과 같이 암·복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고 응용프로그램에서 암·복호화 모듈을 호출하는 방식이다.

❍ DB 서버에는 영향을 주지 않지만 어플리케이션 서버에 암·복호화를 위한 추가적인 부하가 발생하며, 구축 시 응용프로그램 전체 또는 일부 수정이 필요하다.

❍ 추가적으로 어플리케이션 서버와 DB 서버 간의 통신에서 암호화된 개인정보의 전송을 보장할 수 있다.



<그림 8> 응용프로그램 자체 암호화 방식의 개념도

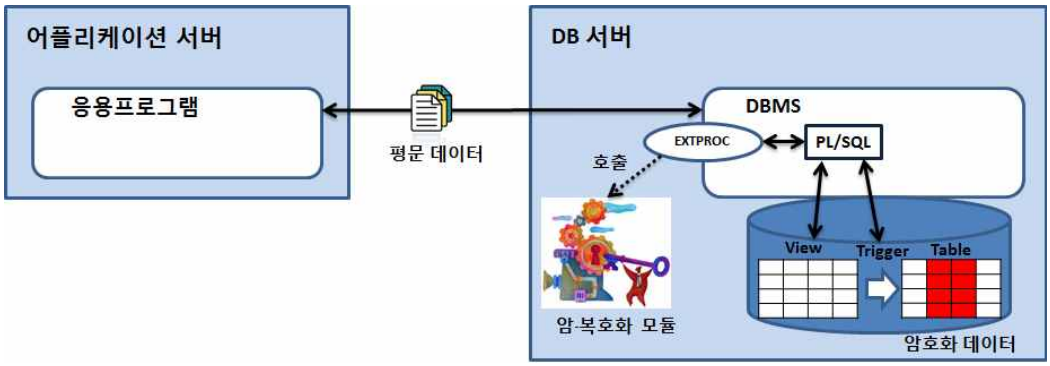
❍ 응용프로그램 자체 암호화 방식의 주요 특성은 [표 6]과 같다.

[표 6] 응용프로그램 자체 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	어플리케이션 서버
암·복호화 요청	응용프로그램
DB 서버의 부하	없음(어플리케이션 서버에 부하 발생)
색인 검색	일치검색 가능 별도 색인 테이블 생성을 통해 가능(추가 작업 필요)
배치 처리	가능
응용프로그램 수정	필요함
DB 스키마 수정	거의 필요하지 않음(암호화에 따른 속성 타입이나 길이의 변경이 필요할 수 있음)

2.1.3 DB 서버 암호화 방식

- DB 서버 암호화 방식은 <그림 9>와 같이 암·복호화 모듈이 DB 서버에 설치되고 DBMS에서 플러그인(plug-in)으로 연결된 암·복호화 모듈을 호출하는 방식이다.
- 응용프로그램의 수정이 거의 필요하지 않아 구현 용이성이 뛰어나지만, 기존 DB 스키마와 대응하는 뷰(view)를 생성하고 암호화할 테이블을 추가하는 작업이 필요하다.
- 어플리케이션 서버의 성능에는 영향을 주지 않지만 DBMS에서 DB 서버의 암·복호화 모듈을 플러그인으로 호출할 때 추가적인 부하가 발생하여 성능이 저하될 수 있다.



<그림 9> DB 서버 암호화 방식의 개념도

- DB 서버 암호화 방식의 주요 특성은 [표 7]과 같다.

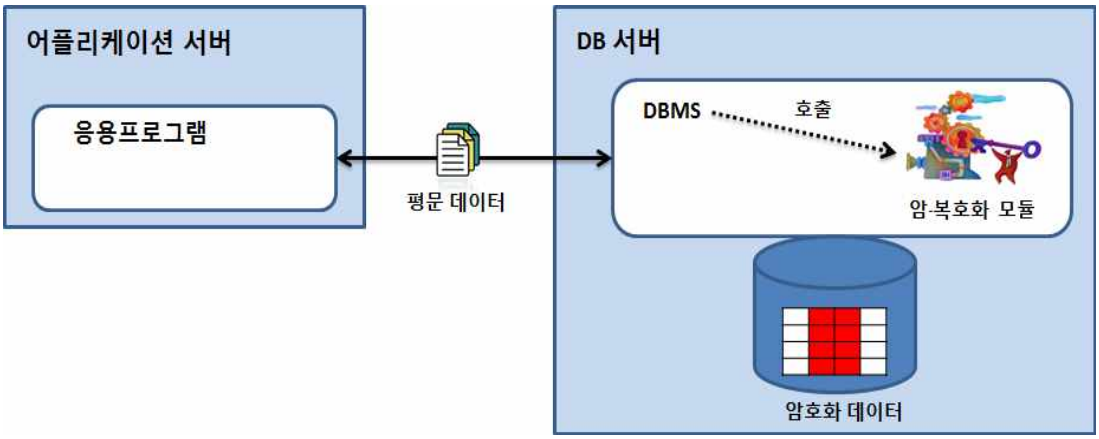
[표 7] DB 서버 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	DB 서버
암·복호화 요청	DB 서버
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능(대량의 배치 트랜잭션 처리는 많이 느릴 수 있음)
응용프로그램 수정	기본적으로 수정 없이 적용할 수 있으나, 제약사항 또는 성능 문제가 있는 경우 수정이 필요함
DB 스키마 수정	필요함

2.1.4 DBMS 자체 암호화 방식

❍ DBMS 자체 암호화 방식은 <그림 10>과 같이 DBMS에 내장되어 있는 암호화 기능(TDE : Transparent Data Encryption)을 이용하여 암·복호화 처리를 수행하는 방식이다.

❍ DBMS 커널 수준에서 처리되므로 기존 응용프로그램의 수정이나 DB 스키마의 변경이 거의 필요하지 않고 DBMS 엔진에 최적화된 성능을 제공할 수 있다.



<그림 10> DBMS 자체 암호화 방식의 개념도

❍ DBMS 자체 암호화 방식의 주요 특성은 [표 8]과 같다.

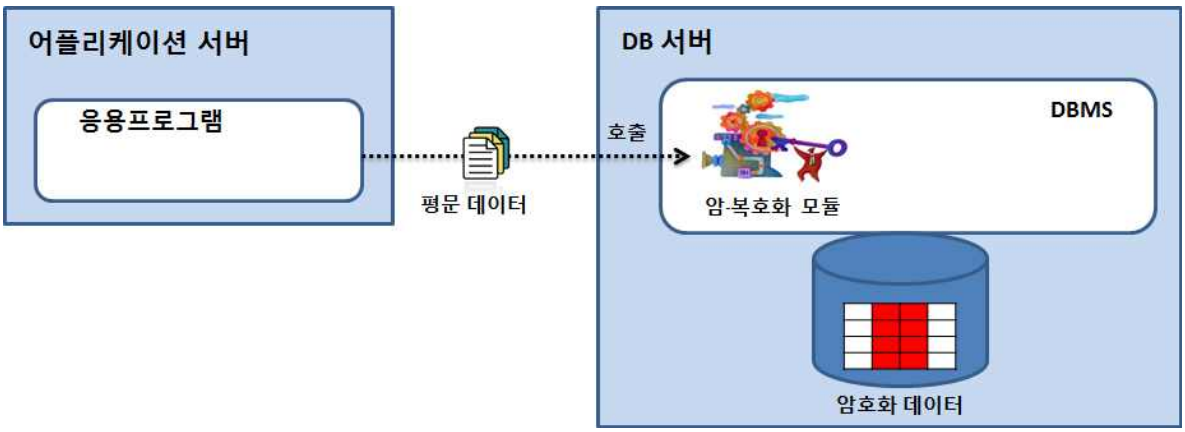
[표 8] DBMS 자체 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	DB 서버
암·복호화 요청	DBMS 엔진
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능
응용프로그램 수정	필요하지 않음
DB 스키마 수정	거의 필요하지 않음(암호화할 DB 스키마 지정 필요)

2.1.5 DBMS 암호화 기능 호출 방식

❍ DBMS 암호화 기능 호출 방식은 <그림 11>과 같이 DBMS가 자체적으로 암·복호화 기능을 수행하는 API를 제공하고 해당 함수를 사용하기 위해 응용프로그램에서 호출하는 방식이다.

❍ 암·복호화 API를 사용하는 응용프로그램의 수정이 필요하고, DB 서버에 추가적인 부하가 발생할 수 있다.



<그림 11> DBMS 암호화 기능 호출 방식의 개념도

❍ DBMS 암호화 기능 호출 방식의 주요 특성은 [표 9]와 같다.

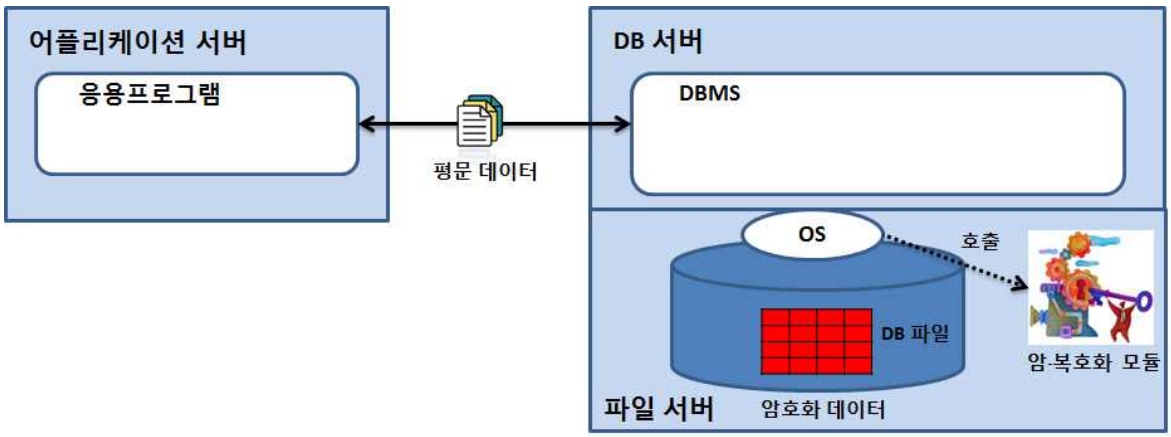
[표 9] DBMS 암호화 기능 호출 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	DB 서버
암·복호화 요청	응용프로그램
DB 서버의 부하	있음
색인 검색	불가능
배치 처리	가능(대량의 배치 트랜잭션 처리는 많이 느릴 수 있음)
응용프로그램 수정	수정 필요
DB 스키마 수정	일부 수정 필요

2.1.6 운영체제 암호화 방식

❍ 운영체제 암호화 방식은 <그림 12>와 같이 OS에서 발생하는 입출력 시스템 호출을 이용한 암·복호화 방식으로서 DB 파일 자체를 암호화한다.

❍ 응용프로그램이나 DB 스키마의 수정이 필요하지 않지만 DB 파일 전체를 암호화하는데 따른 파일 서버 및 DB 서버에 추가적인 부하가 발생할 수 있다.



<그림 12> 운영체제 암호화 방식의 개념도

❍ 운영체제 암호화 방식의 주요 특성은 [표 10]과 같다.

[표 10] 운영체제 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	파일 서버(또는 DB 서버)
암·복호화 요청	운영체제
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능
응용프로그램 수정	필요하지 않음
DB 스키마 수정	필요하지 않음

2.2 업무용 컴퓨터 암호화

2.2.1 개요

❍ 업무용 컴퓨터에서는 보조저장매체에 저장된 개인정보의 보호를 위하여 개별 문서 파일 단위로 암호화(파일 암호화) 또는 디렉터리 단위로 암호화(디스크 암호화)를 수행해야 한다.

❍ 파일 암호화는 업무용 컴퓨터에 저장된 개인정보에 대한 보호뿐만 아니라 개인정보취급자 간에 네트워크상으로 파일을 안전하게 전송하기 위한 방식으로도 사용할 수 있다.

❍ 업무용 컴퓨터에서 가능한 암호화 방식은 [표 11]과 같이 구분할 수 있다.

[표 11] 업무용 컴퓨터 암호화 방식의 구분

방식	주요 내용
문서 도구 자체 암호화	• 업무용 컴퓨터에서 사용하는 문서도구의 자체 암호화 기능을 통하여 개인정보 파일 암호화
암호 유틸리티를 이용한 암호화	• 업무용 컴퓨터의 OS에서 제공하는 파일 암호 유틸리티 또는 파일 암호 전용 유틸리티를 이용한 개인정보 파일의 암호화
DRM (Digital Right Management)	• DRM을 이용하여 다양한 종류의 파일 및 개인정보 파일의 암호화
디스크 암호화	• 디스크에 데이터를 기록할 때 자동으로 암호화하고, 읽을 때 자동으로 복호화하는 기능을 제공함 • 디스크 전체 또는 일부 디렉터리를 인가되지 않은 사용자에게 보이지 않게 설정하여 암호화 여부와 관계없이 특정 디렉터리 보호 가능

❍ 업무용 컴퓨터 암호화 방식의 특징을 간단히 비교하면 [표 12]와 같다.

[표 12] 업무용 컴퓨터 암호화 방식의 비교

방식	지원 파일 종류	
	특정 문서*	일반 파일**
문서 도구 자체 암호화	지원함	지원하지 않음
암호 유틸리티를 이용한 암호화	지원함	지원함
DRM	지원함	지원함
디스크 암호화	지원함	지원함

*특정문서: 흔히 사용하는 문서 도구(예: ㅎ글, MS 워드 등)로 작성한 파일
**일반문서: 특정 문서 이외의 문서(예: 텍스트 파일, 이미지 파일 등)

2.2.2 문서 도구 자체 암호화 방식

❍ 업무용 컴퓨터에서 주로 사용하는 문서 도구(예를 들어, 흔글, MS 워드 등)에서는 자체 암호화 기능을 통하여 개인정보 파일을 암호화할 수 있다.

2.2.3 암호 유틸리티를 이용한 암호화 방식

❍ 업무용 컴퓨터에서는 해당 컴퓨터의 OS에서 제공하는 파일암호 유틸리티 또는 파일암호 전용 유틸리티를 이용하여 개인정보 파일 또는 디렉터리를 암호화할 수 있다.

2.2.4 DRM 방식

❍ DRM은 조직 내부에서 생성되는 전자문서를 암호화하고 해당 문서를 접근 및 사용할 수 있는 권한을 지정함으로써 허가된 사용자만 중요 문서(개인정보 문서, 기밀문서 등)를 사용하게 하는 기술이다.

❍ DRM은 중요 문서 외에 다양한 종류의 멀티미디어 콘텐츠(음악, 사진, 동영상, 이미지 등)에 대한 보안 기능을 제공할 수 있다.

❍ DRM으로 암호화된 문서는 DRM 클라이언트가 없는 PC에서는 열람이 불가능하며, 열람 중에도 파일이 복호화 되지 않고 암호화 상태를 유지한다.

2.2.5 디스크 암호화 방식

❍ 디스크 암호화는 디스크에 데이터를 기록할 때 자동으로 암호화하고, 주기억장치로 읽을 때 자동으로 복호화하는 방식이다.

❍ 휴대용 보조기억매체는 개방된 장소에 놓일 수 있기 때문에 적절한 물리적 보안을 제공하기 어려움이 있다. 따라서 휴대용 보조기억매체는 저장된 개인정보의 기밀성을 위해 디스크 암호화 솔루션을 이용하여 암호화하기를 권고한다.

Ⅳ 개인정보 암호화 적용 사례

제1절 전송시 암호화

1.1 웹서버와 클라이언트 간 암호화 사례

1.1.1 아파치(Apache) 웹서버를 이용한 SSL 방식의 설정

- 대표적인 오픈소스 웹서버 소프트웨어인 아파치에서 설정파일인 'httpd.conf'를 변경하여 SSL/TLS를 설정할 수 있다. 이 설정파일에는 공인인증서의 위치, 서버용 인증서 위치, 공개키와 개인키의 위치 등이 들어가며 SSL/TLS에서 사용하는 암호 알고리즘을 정해준다.
- 웹브라우저가 SSL 방식으로 웹서버에 연결된 경우, <그림 13>과 같이 웹브라우저 주소창 또는 하단의 상태표시줄에 자물쇠 표시가 나타나게 된다.

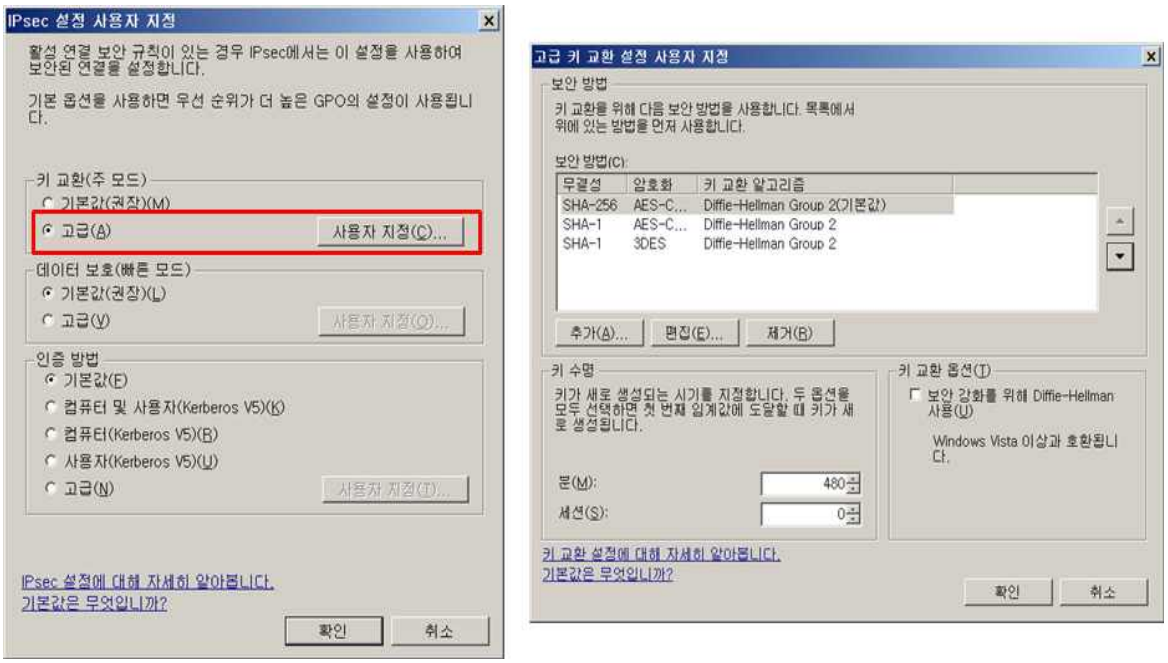
<그림 13> SSL 방식에서 나타나는 웹브라우저 자물쇠 표시

1.2 개인정보처리시스템 간 암호화 사례

1.2.1 윈도우(Windows)에서 IPsec VPN 방식의 설정

- 윈도우를 호스트로 사용하여 IPsec VPN에 접속할 경우, 안전한 암호 알고리즘의 선택을 위해 추가 설정이 필요할 수 있다.
- Windows 7의 제어판 메뉴에서 [윈도우 방화벽] → [고급설정] → [로컬 컴퓨터 고급 보안이 포함된 윈도우 방화벽] → [속성] → [IPsec 설정] → [사용자 지정]을 선택한다.

❍ <그림 14>의 [IPsec 설정 사용자 지정]과 같은 대화창이 나타나면, [키 교환] → [사용자 지정]을 선택하여 [고급 키 교환 설정 사용자 지정]에서 IPsec VPN 방식에 사용할 암호 알고리즘을 변경할 수 있다.



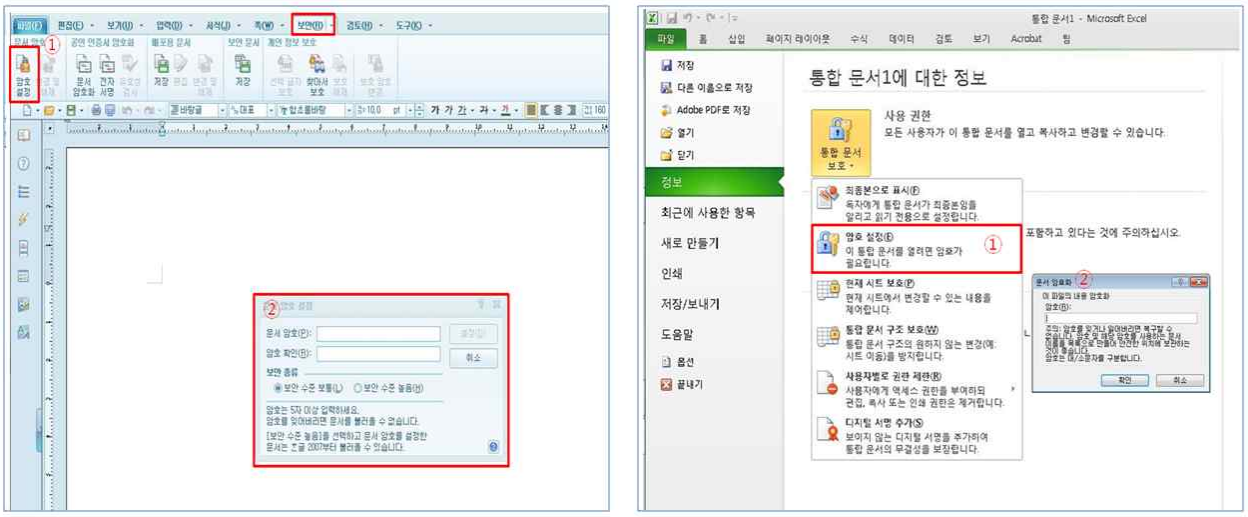
<그림 14> Windows 7에서 IPsec VPN 방식을 위한 암호 알고리즘 설정

1.3 개인정보취급자 간 암호화 사례

1.3.1 첨부문서 암호화 후, 이메일로 전송

❍ 먼저, 응용프로그램의 암호화 기능을 사용하여 암호를 설정한 후, 문서를 저장한다.

- 혼글 2010의 경우, 상단 메뉴의 [보안] → [문서 암호 설정]을 이용하여 문서의 암호를 설정 한 후, [파일] → [저장하기] 메뉴를 이용하여 문서 내용을 저장한다.
- MS 엑셀 2010의 경우 상단 메뉴의 [파일] → [정보] → [통합 문서 보호] → [암호 설정]을 이용하여 문서의 암호를 설정 한 후, [파일] → [저장하기] 메뉴를 이용하여 문서의 내용을 저장한다.



<그림 15> 흔글 2010과 MS 엑셀 2010에서 문서 암호화 설정

❍ 암호화된 문서를 이메일에 첨부한 후, 수신자에게 이메일을 전송한다.

제2절 저장시 암호화

2.1 개인정보처리시스템 암호화 사례

2.1.1 응용프로그램 자체 암호화 방식

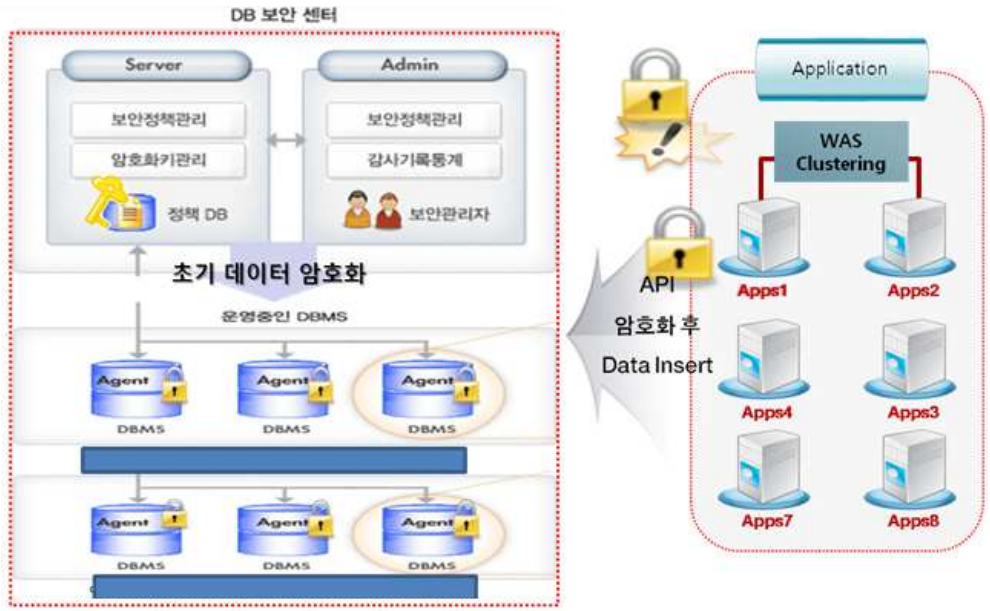
❍ 적용 환경

- 적용분야: 공공기관
- 업무종류: OO기관 대국민서비스
- 개인정보보유량: 약 9천3백만 건

❍ 적용 사유

- 차세대 시스템으로 새로운 응용프로그램 개발이 필요함
- 기존 DBMS에서 플러그인을 제공하지 않음

❍ 적용 구성도



<그림 16> 응용프로그램 자체 암호화 방식의 적용 구성도

❍ 주요 특징

- 암·복호화 작업이 다수의 어플리케이션 서버로 부하 분산
- 암호화 컬럼 크기 증가에 따라 관련 응용프로그램 인터페이스의 변경이 필요
- 암호화 후 DB 서버의 성능 저하는 적으나, 일부 질의에서는 색인 처리 불가로 응용프로그램 코드의 변경이 요구
- 암호화 컬럼 크기 증가에 따른 DB 서버 디스크 및 주기억장치 증설 필요
- 암·복호화 작업 부하에 따라 자원 여유율이 매우 작은 응용 서버(예 : WAS)는 자원 증설이 요구

2.1.2 DB 서버 암호화 방식

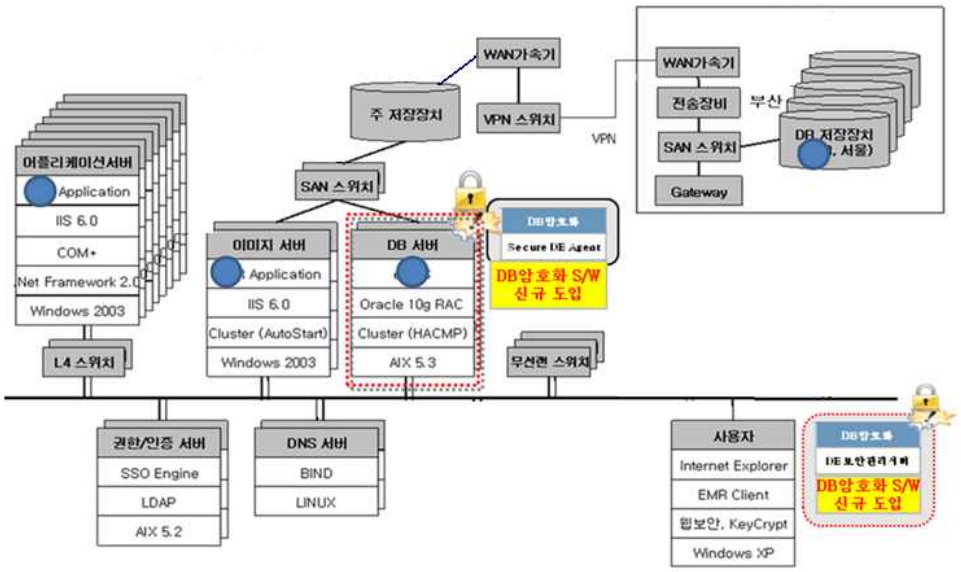
❍ 적용 환경

- 적용분야: 공공기관
- 업무종류: OO기관 통합정보시스템
- 개인정보보유량: 약 1억 건

❍ 적용 사유

- 운영 중인 응용프로그램 및 패키지 응용프로그램 수정을 최소화하여 단기간에 개발이 필요함
- 기존 DBMS에서 플러그인 기능을 제공함
- DB 서버의 성능 저하가 발생할 만한 복잡한 트랜잭션이나 배치 업무가 적음

❍ 적용 구성도



<그림 17> DB 서버 암호화 방식의 적용 구성도

❍ 주요 특징

- 암·복호화 작업이 DB 서버에 집중됨으로써 해당 서버의 자원 (CPU 및 주기억장치) 사용률 증가
- 암·복호화 뷰(암호화 이전 테이블명과 동일)와 트리거 구조를 이용하여 응용프로그램 변경 최소화
- 암호화 컬럼 크기 증가에 따라 관련 응용프로그램 인터페이스의 변경 필요
- 암호화로 인한 DB 성능 저하를 최소화하기 위하여 DB 질의와 응용프로그램의 튜닝 필요
- 암호화 컬럼 크기 증가와 암·복호화 작업 부하로 인해 DB 서버에 CPU 및 주기억장치, 디스크 증설 필요

2.1.3 DBMS 자체 암호화 방식

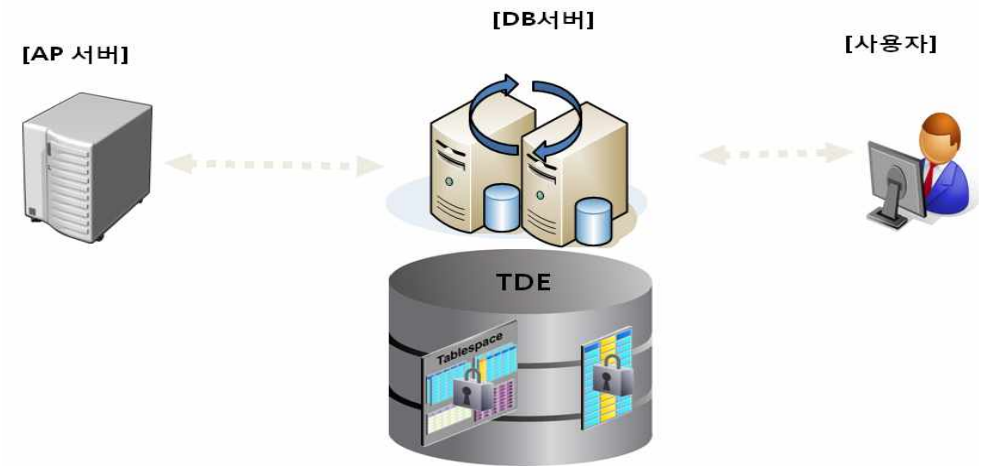
❍ 적용 환경

- 적용분야: 민간기관
- 업무종류: OO병원 수납시스템
- 개인정보보유량: 약 3억8천만 건

❍ 적용 사유

- 개발 인력의 부족으로 기존 응용프로그램의 수정을 최소화해야 함
- 대량 개인정보의 안정적인 처리가 필요함

❍ 적용 구성도



<그림 18> DBMS 자체 암호화 방식의 적용 구성도

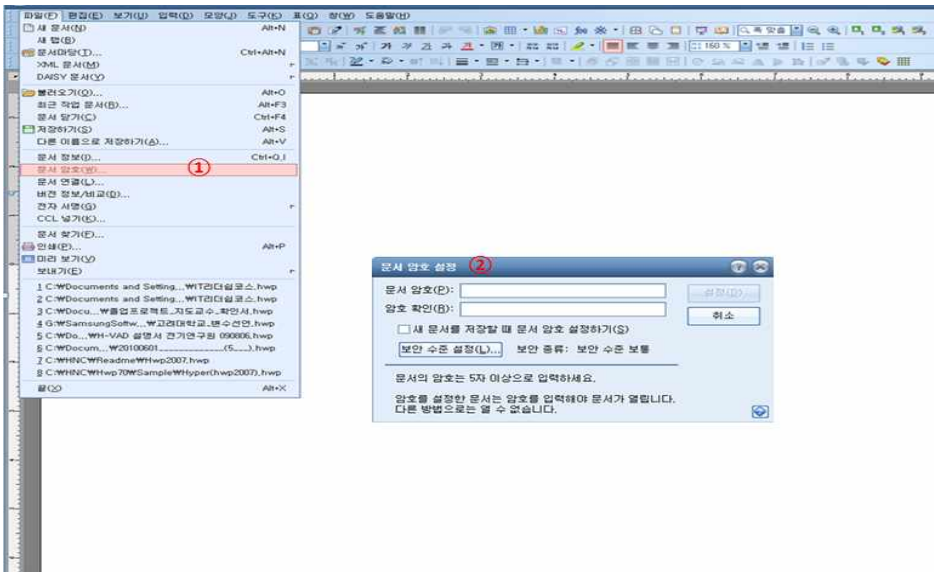
❍ 주요 특징

- DB 커널에서 암·복호화를 수행하므로 DB 서버의 CPU, 주기억장치, 디스크 등의 추가적인 부하가 적음
- 응용프로그램의 변경이 없으며, ERP 등 패키지에 암호화 적용 가능
- 암호화 테이블과 기존 테이블의 관리 도구 일원화로 운영 편의성 제공
- 비밀번호 일방향 암호화를 위한 암·복호화 모듈의 추가 필요

2.2 업무용 컴퓨터 암호화 사례

❍ 흔글 2007 문서 암호화 예제

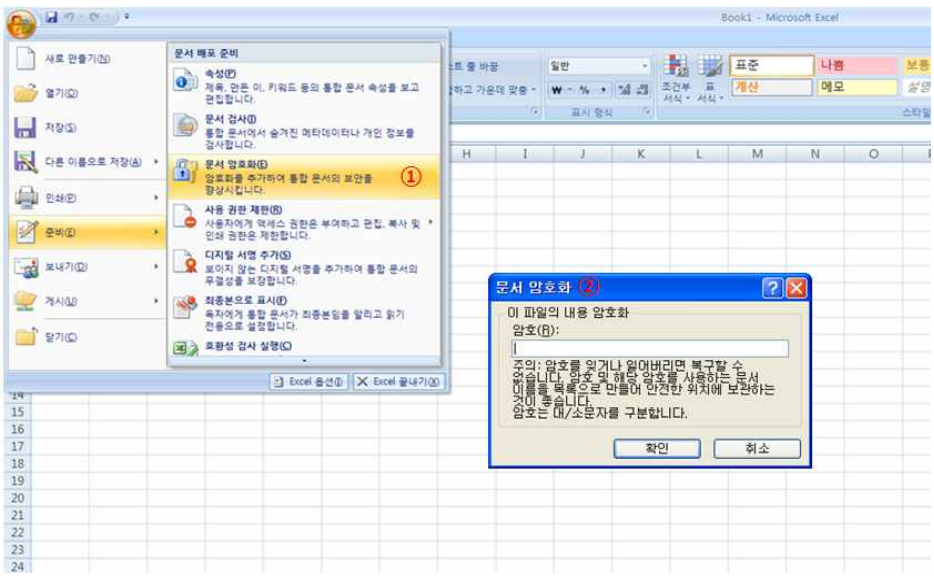
▪ [파일] → [문서암호] (흔글 2010의 경우: [보안] → [문서암호 설정])



<그림 19> 흔글 2007을 이용한 문서 암호화 적용

❍ MS 엑셀 2007 문서 암호화 예제

▪ [오피스 단추] → [준비] → [문서암호화] (MS 엑셀 2010의 경우 : [파일] → [정보] → [통합 문서 보호] → [암호 설정])



<그림 20> MS 엑셀 2007을 이용한 문서 암호화 적용

Ⅴ FAQ

【Q1】 공공기관이 아닌 일반기업입니다. 개인정보처리시스템의 DBMS (DataBase Management System)에서 제공하는 TDE(Transparent Data Encryption) 방식을 사용한 암호화가 개인정보보호법에 위배됩니까?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 고유식별정보 암호화시 안전한 알고리즘을 사용하도록 하고 있습니다. TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반 사항이 아닙니다.

【Q2】 공공기관입니다. 개인정보처리시스템의 DBMS(DataBase Management System)에서 제공하는 TDE(Transparent Data Encryption) 방식을 사용한 암호화가 개인정보보호법에 위배됩니까?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 암호화시 안전한 알고리즘을 사용하도록 하고 있으므로, TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반은 아닙니다.

다만, 공공기관은 전자정부법에 따라 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용하여야 합니다.

※ 자세한 사항은 "국가 정보보안 기본지침"을 확인하시기 바랍니다.

【Q3】 금융기관입니다. 개인정보처리시스템인 DBMS가 제공하는 TDE (Transparent Data Encryption) 방식을 사용한 암호화가 개인정보 보호법에 위배됩니까?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 암호화시 안전한 알고리즘을 사용하도록 하고 있으므로, TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반은 아닙니다.

다만, 전자금융감독규정에서 금융기관 또는 전자금융업자는 국가기관의 평가·인증을 받은 장비를 사용하도록 하고 있으므로 이를 확인하여야 합니다.

※ 자세한 사항은 "전자금융감독규정"을 확인하시기 바랍니다.

【Q4】 안전한 암호 알고리즘이 무엇인가요?

안전한 암호 알고리즘은 국내외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)에서 권고하고 있는 알고리즘을 의미합니다. 본 안내서의 '[표 1] 안전한 암호 알고리즘(예시)'를 참고하시기 바랍니다.

※ 공공기관은 IT보안인증사무국(http://service1.nis.go.kr)의 검증필 암호 모듈 또는 제품 참조

※ 암호기술 구현 안내서(2011.11, 한국인터넷진흥원). 암호 알고리즘 및 키 길이 이용 안내서(2009.3, · 한국인터넷진흥원)

【Q5】 주민등록번호를 저장하면 무조건 암호화해야 하나요?

인터넷에서 직접 접근이 가능한 구간(인터넷망, DMZ 구간)에 위치한 개인정보처리시스템에 주민등록번호를 저장하면 반드시 암호화해야 하며, 물리적인 망분리, 방화벽 등으로 분리된 내부망에 고유식별정보를 저장하는 경우에는 암호화 기술을 적용하거나 또는 암호화에 상응하는 조치를 할 수 있습니다.

※ '암호화에 상응하는 조치'란 「**개인정보 위험도 분석기준**」에 따라 보호조치를 이행하는 경우를 의미함 (개인정보 위험도 분석기준 및 해설서(행정안전부 공고 제2012-112)는 www.privacy.go.kr에서 다운로드)

【Q6】 DB에 저장된 주민등록번호를 일부분만 암호화해서 저장해도 되는 것인지요?

예, 일부분 암호화가 가능합니다. 시스템 운영이나 개인 식별을 위해 해당 정보를 활용해야 하는 경우 생년월일 및 성별을 포함한 앞 7자리를 제외하고 뒷자리 6개 번호를 암호화 하여 사용하실 수 있습니다.

(예:000000-1******)

【Q7】 DB에 외국인등록번호와 주민등록번호를 저장하고 있습니다. 둘 다 전체 암호화해서 저장해야 하나요?

외국인등록번호만 저장하는 경우에는 전체 암호화해야합니다. 외국인등록번호와 주민등록번호가 혼재되어 저장하는 경우에는 외국인등록번호 뒷부분 6자리만 암호화해도 무방합니다.

【Q8】 안전한 알고리즘이 다양한 키 길이를 제공하고 있는데, 키 길이에 상관없이 아무거나 사용해도 되나요?

암호 알고리즘은 키 길이 등에 따른 안전성 유지기간을 가지고 있으므로, 키 길이가 128 비트 미만인 대칭키 암호화 알고리즘과 해쉬값 길이가 112 비트 이하의 일방향 암호 알고리즘은 사용하지 않도록 권고합니다.

【Q9】 회사에 고객들의 이름, 주소, 전화번호, e-mail, 비밀번호를 저장하고 있습니다. 암호화 대상이 무엇인가요?

개인정보의 안전성 확보조치 기준 고시 제7조에서 암호화 대상은 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보입니다. 따라서 이 경우에는 비밀번호만 일방향 암호화해서 저장하시면 됩니다.

【Q10】 부동산중개업을 하고 있습니다. 업무용 컴퓨터에 ㅎ글, 엑셀을 이용하여 주민등록번호를 처리하고 있습니다. 암호화를 어떻게 해야 합니까?

ㅎ글, 엑셀 등을 이용하여 주민등록번호를 처리하는 경우 해당 프로그램에서 제공하는 비밀번호 설정 기능을 사용하여 암호화를 적용하시면 됩니다.

※ 업무용 프로그램에서 제공하는 비밀번호를 사용하는 경우 해당 프로그램에서 제공하는 암호화 알고리즘의 안전성을 확인하시기 바랍니다.

【Q11】 개인정보처리시스템을 위탁하거나, ASP(Application Service Provider)를 이용하는 경우 암호 수행을 위탁기관에서 해야 하는지 아니면 수탁기관에서 해야 하는지?

개인정보의 암호화 등 안전성확보조치는 원칙적으로 "개인정보처리자"의 의무입니다. 따라서 개인정보처리시스템을 위탁하거나 ASP를 이용하는 경우에도 암호화 조치사항에 대한 이행여부에 대한 책임은 위탁기관이 지게 됩니다.

다만, 위탁기관은 암호화에 대한 요구사항을 수탁기관과의 계약서 등에 명시하여 수탁기관으로 하여금 처리하게 요구할 수 있습니다.

[붙임 1] 국가정보원(IT보안인증사무국) 검증대상 암호알고리즘 목록

분류		암호알고리즘	참조표준
블록암호		ARIA SEED	KS X 1213-1(2009) KS X 1213-2(2009) TTAS.KO-12.0004/R1(2005) TTAS.KO-12.0025(2003)
해쉬함수		SHA-224 SHA-256 SHA-384 SHA-512	ISO/IEC 10118-3(2004) ISO/IEC 10118-3 Amd1(2006)
메시지 인증코드	해쉬함수 기반	HMAC	ISO/IEC 9797-2(2011)
	블록암호 기반	GCM(GMAC) CCM, CMAC	KS X 1213-2(2009) ISO/IEC 9797-1(2011) TTAK.KO-12.0131(2010)
난수발생기	해쉬함수/ HMAC기반	Hash_DRBG HMAC_DRBG	ISO/IEC 18031(2011) NIST SP 800-90
	블록암호 기반	CTR_DRBG	
키 설정 방식		DH ECDH	ISO/IEC 11770-3(2008) NIST FIPS 186-3
공개키 암호		RSAES	ISO/IEC 18033-2(2006)
전자서명		RSA-PSS, KCDSA, ECDSA, EC-KCDSA	ISO/IEC 14888-2(2008) ISO/IEC 14888-3(2006) TTAS.KO-12.0001/R1(2000) TTAS.KO-12.0015(2001) NIST FIPS 186-3

[붙임 2] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

□ 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

제7조(개인정보의 암호화)

① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 제3항, 제4항 및 제5항에 따른 개인정보 저장시 암호화를 적용하는 경우, 이 기준 시행일로부터 3개월 이내에 다음 각 호의 사항을 포함하는 암호화 계획을 수립하고, 2012년 12월 31일까지 암호화를 적용하여야 한다. 단 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우 위험도 분석과 관계없이 암호화를 적용하여야 한다.

1. 개인정보의 저장 현황분석
2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법
3. 암호화 추진 일정 등

⑧ 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

□ 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화) 해설

> ① 영 제21조 및 영 제30조에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

■ "고유식별정보"는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며, 대통령령으로 주민등록번호, 여권번호, 면허번호, 외국인등록번호 등을 정하고 있다.

■ "비밀번호"는 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

■ "바이오정보"는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

> ② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

■ 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보 등 정보통신망 내외부로 송·수신할 모든 개인정보에 대해서는 암호화하여야 한다.

· 내부망 내에서 송·수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화하여야 한다.
· 전용선을 이용하여 개인정보를 송·수신하는 경우, 암호화가 필수는 아니나 내부자에 의한 개인정보 유출 등을 대비해서 가급적 암호화 전송을 권장한다.

■ 개인정보 암호화 전송을 위해 보안서버를 활용할 수 있다.

· "보안서버"란 웹서버에 SSL(Secure Sockets Layer) 인증서나 암호화 소프트웨어를 설치하여 암호통신을 수행하는 방식을 말한다.

■■■ 보안서버 구축방식 예시 ■■■

〈SSL 방식의 보안서버 실행 확인〉

〈응용프로그램 방식의 보안서버 실행 확인〉

■ "보조저장매체"는 컴퓨터에 장착된 하드디스크(HDD) 등의 저장매체 이외에 전자적으로 자료를 저장할 수 있는 매체로서 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓, 자기 테이프 등 개인정보처리시스템, 업무용 컴퓨터 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.

- 이러한 매체에 개인정보를 저장 후 분실할 경우, 개인정보가 노출될 위험이 있으므로, 암호화 기능을 제공하는 보조저장매체를 사용하거나 개인정보를 암호화 저장하여 분실되더라도 다른 사람이 알 수 없도록 조치하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

■ 개인정보처리자는 비밀번호, 바이오정보(지문, 홍채 등)가 노출 또는 위·변조되지 않도록 암호화 하여 저장하여야 하며, 특히 비밀번호의 경우에는 복호화되지 않도록 일방향 (해쉬함수) 암호화 하여야한다.

■ 일방향 암호화는 저장된 값으로 원본값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.

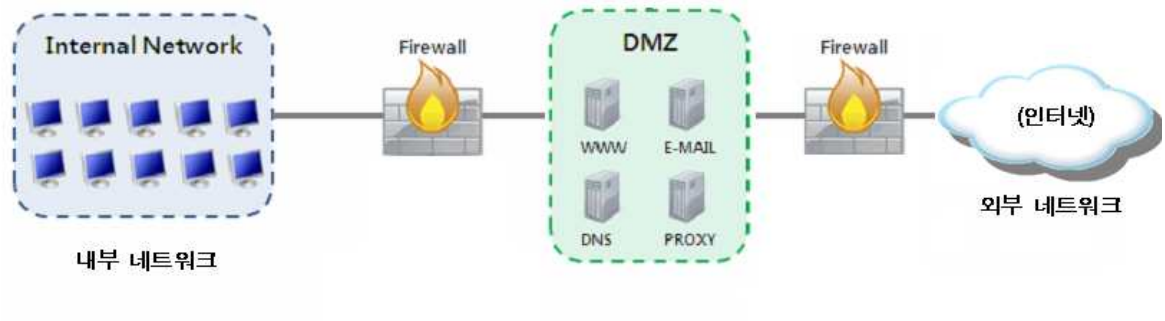
■■■ 일방향(해쉬 함수) 암호화 ■■■

- 일방향(해쉬 함수) 암호화는 입력된 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 길이가 고정된 결과를 만들어 내는 방법을 의미한다.
- 일방향(해쉬 함수) 암호화의 가장 기본적인 성질은 두 해쉬 결과가 다르다면 원래의 데이터도 어딘가 다르다는 것을 의미하며, 원래 입력의 한 비트만 바뀌더라도 해쉬 결과는 크게 달라지기 때문에 전자서명 방식에 이용되고 있다.

■ 바이오 정보의 경우, 복호화가 가능한 양방향 암호화 저장이 필요하나, 이는 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외된다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

■ 인터넷 구간은 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간, DMZ 구간은 인터넷과 내부망과 인터넷 구간 사이에 위치한 중간 지점으로 침입차단시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말한다. 내부망은 접근통제시스템 등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역을 말한다.



■ 인터넷 구간이나 DMZ 구간은 외부에서 직접 접근이 가능하므로 외부자의 침입을 받을 가능성이 있다. 이에 따라 DMZ 구간에 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등의 고유식별정보를 저장하는 경우 암호화하여 저장해야 한다. 제2항에 따른 비밀번호 및 바이오 정보를 저장하는 경우에도 암호화하여 저장해야한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 결정할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

■ 내부망에 고유식별정보를 저장하는 경우, 개인정보 영향평가 및 위험도 분석 결과에 따라 암호화 적용여부 및 적용범위를 결정하여 시행할 수 있다.

- 영 제35조에 따라 영향평가의 대상이 되는 공공기관은 해당 개인정보 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정한다.
- 개인정보 영향평가의 실시대상이 아니거나 공공기관 이외의 개인정보처리자는 위험도 분석을 실시한 후 그 결과에 따라 고유식별정보의 암호화 적용여부 및 적용범위를 정하여 시행한다.

· 개인정보 영향평가 수행을 위한 교육교재 참조

■ "위험도 분석"은 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

- 세부적으로 위험도 분석은 개인정보 유출에 영향을 미칠 수 있는 다양한 위협에 대한 시스템 취약점과 이로 인해서 예상되는 손실을 분석하여 위험요소를 식별, 평가하고 그러한 위험요소를 적절하게 통제할 수 있는 수단을 체계적으로 구현하고 운영하는 전반적인 행위 및 절차로서 위험관리의 일부분이다.

■ "위험도 분석"은 개인정보를 저장하는 정보시스템에서 개인정보파일 단위로 수행하고 각 개별 개인정보파일의 위험점수에 따라 개별 개인정보파일 단위로 암호화 여부를 결정해야하며, 위험도 분석을 수행한 결과는 최고경영층으로부터 내부결재 등의 승인을 받아야 한다.

· 위험도 분석 점검표 참조

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

■ "안전한 암호 알고리즘"이란 미국 NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 및 국내외 암호 연구기관에서 권고하는 알고리즘을 의미한다.

· 고유식별정보, 바이오 정보는 원칙적으로 암호화해야 하나, 시스템 운영이나 개인 식별을 위해 해당 개인정보를 활용하는 경우 암호화/복호화에 대한 부하가 발생할 수 있다. 이 경우, 주민등록번호 등과 매핑하여 임의의 서비스 번호를 부여해서 사용할 수 있으며 임의의 서비스번호와 매핑되는 주민등록번호는 암호화하여 저장·관리하여야 한다.

■ 주민등록번호를 시스템 운영을 위한 검색 키로 사용하는 경우, 속도 등 성능을 고려하여 일부 정보만 암호화 조치를 취할 수 있다.

※ 주민등록번호의 경우 뒷자리 6개 번호 이상 암호화 조치 필요(예시: 700101-1#……&)

⑦ 개인정보처리자는 제3항, 제4항 및 제5항에 따른 개인정보 저장시 암호화를 적용하는 경우, 이 기준 시행일로부터 3개월 이내에 다음 각 호의 사항을 포함하는 암호화 계획을 수립하고, 2012년 12월 31일까지 암호화를 적용하여야 한다. 단 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우 위험도 분석과 관계없이 암호화를 적용하여야 한다.

1. 개인정보의 저장 현황분석
2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법
3. 암호화 추진 일정 등

■ 개인정보처리자가 고유식별번호, 비밀번호, 바이오 정보를 처리하는 경우, 제3항, 제4항 및 제5항에서 규정한 암호화 시행을 위해, 조직 내 의사결정권자의 승인을 득한 암호화 계획을 수립하여 2012년 12월 31일까지 적용하여야 한다.

■■■ 암호화 계획 주요내용 ■■■

1. 개인정보의 저장 현황분석

· 비밀번호, 바이오정보, 고유식별정보를 저장하는 경우에는 암호화의 대상이 되므로 암호화 방법을 결정하기 위해, 개인정보처리자는 제공하는 각 서비스별로 저장하는 개인정보의 종류, 규모, 보유·이용 기간 등의 현황과 이들 서비스를 위해 처리되는 개인정보 보호를 위한 관리적·기술적 보호조치 현황을 분석하여야 한다.

2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법

· 개인정보 영향평가 실시 대상에 따라 개인정보 영향평가를 실시해야 하는 경우에는 영향평가 절차 및 방법을 그 외에 공공기관이나 개인정보처리자는 위험도 분석 절차 및 방법을 작성하여야 한다.
※ 영향평가·위험도 분석 절차 및 방법은 본 기준의 제7조 5항 참조

3. 암호화 추진 일정 등

· 영향평가·위험분석 시행시기 및 암호화 구축 시기 등을 포함한 세부 추진 일정 등을 작성하여야 한다.

· 법 시행 이후 주민등록번호 등 암호화 대상이 포함된 개인정보를 개인정보처리시스템을 신규로 구축하는 경우, 암호화를 즉시 이행하여야 한다.

⑧ 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

■ 고유식별정보를 업무용 컴퓨터에 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려 받아 저장할 때는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 한다.