

개인정보의 암호화 조치 안내서

2017년 1월



본 안내서는 「개인정보 보호법」에 따라 개인정보처리자가 개인정보를 안전하게 저장·전송하는데 사용되는 기술인 암호화에 대한 안내를 제공하고 있습니다.

본 안내서는 개인정보처리자가 고유식별정보, 비밀번호, 바이오정보 등 암호화 대상 개인정보의 저장·전송 시 적용할 수 있는 암호 알고리즘, 수행방식, 사례 등을 제시하고 있으며 제시된 암호 알고리즘 등은 2016년 9월 기준으로 작성되었습니다.

암호 알고리즘 등의 안전성은 시간이 경과하면서 변할 수 있으므로 권고하는 암호 알고리즘 등에 대해서는 국내·외 암호 관련 연구기관에서 제시하는 최신 정보를 확인하시기 바랍니다.

또한 본 안내서에서 제시하는 암호화 적용 사례는 개인정보처리자별 개인 정보처리시스템의 구성 및 운영 환경 등에 따라 적용방식이 달라질 수 있습니다.

[제·개정 이력]

순번	제·개정	주요내용
1	2012. 10.	개인정보 암호화 조치 안내서 발간
2	2017. 1. (개정)	암호 알고리즘별 안전성, 암호 키 관리, 암호화 추진 절차 및 사례 제시 등

Contents



I. 개요

제1절 목적	8
제2절 적용 대상	8
제3절 용어 정의	9

II. 암호화 종류 및 제도

제1절 암호화 종류 및 특성	14
제2절 안전한 암호 알고리즘	16
제3절 암호화 근거 법률	17

III. 암호화 구현 및 키 관리

제1절 전송시 암호화	24
제2절 저장시 암호화	32
제3절 암호키 관리	42

IV. 암호화 추진 절차 및 사례

제1절 암호화 추진 절차	51
제2절 전송시 암호화 사례	63
제3절 저장시 암호화 사례	65

V. 부록

제1절 FAQ	76
제2절 참고자료	79

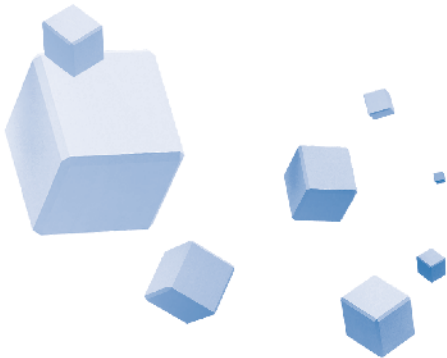
I.

개요

제1절 목적


제2절 적용 대상

제3절 용어 정의



I. 개요

제1절 목적


 본 안내서는 「개인정보 보호법」에 따라 개인정보처리자가 개인정보를 안전하게 저장·전송하는데 사용되는 암호화 기술에 대한 안내를 목적으로 한다.

이를 위해 본 안내서는 개인정보처리자가 고유식별정보, 비밀번호, 바이오정보 등 암호화 대상 개인정보의 저장·전송 시 적용할 수 있는 암호 알고리즘을 소개하고 개인정보처리자의 효과적인 암호화 적용을 지원하기 위해 암호화 적용 방식 및 절차, 암호화 적용 시 고려사항, 암호화 적용 사례 등을 제시한다.











개인정보 보호법 - 암호화 관련 근거


- 「개인정보 보호법」 제24조(고유식별정보의 처리제한) 및 동법 시행령 제21조(고유식별정보의 안전성 확보 조치)
- 「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한) 및 동법 시행령 제21조의2(주민등록번호 암호화 적용 대상 등)
- 「개인정보 보호법」 제29조(안전조치의무) 및 동법 시행령 제30조(개인정보의 안전성 확보조치)
- 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2016-35호)


제2절 적용 대상


 「개인정보 보호법」에 따라 암호화하여야 하는 개인정보인 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 저장·전송하는 개인정보처리자를 대상으로 한다.


제3절 용어 정의


-  “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
-  “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
-  “개인정보처리자”란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
-  “개인정보취급자”는 개인정보처리자의 지휘, 감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
-  “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
-  “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템을 말한다.
-  “내부망”이란 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
-  “비밀번호”란 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”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 말한다.
-  “보조저장매체”란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.


-  “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.


-  “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.


-  “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.


-  “암호화”란 일상적인 문자로 쓰이는 평문을 암호키를 소유하지 않은 사람이 알아볼 수 없도록 기호 또는 다른 문자 등의 암호문으로 변환하는 것을 말한다. 개인정보가 비인가자에게 유·노출 되더라도 그 내용을 확인할 수 없거나 어렵게 하는 보안기술이다.


-  “암호키”란 메시지를 암호화 또는 복호화 하는데 사용되는 키로서 암호키를 소유한 자만이 암호문을 생성하거나 복호할 수 있다.

-  “해쉬함수”란 임의의 길이의 메시지를 항상 고정된 길이의 해쉬 값으로 변환하는 일방향 함수를 말한다.

-  “일방향 함수”라 함은 결과값을 가지고 입력값을 구하는 것이 어려운 함수로서 해쉬함수는 일방향 함수에 해당한다.

-  “블록암호”란 평문을 일정한 블록 크기로 나누어 각 블록을 송·수신자 간에 공유한 비밀키를 사용하여 암호화 하는 방식이다.

-  “SSL(Secure Sockets Layer)”이란 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜을 말한다.

-  “가상사설망”(VPN : Virtual Private Network)은 정보통신망에서 IPsec, SSL 등의 보안 프로토콜을 사용한 터널링 기술을 통해 안전한 암호화 통신을 할 수 있도록 해주는 보안 시스템을 말한다.

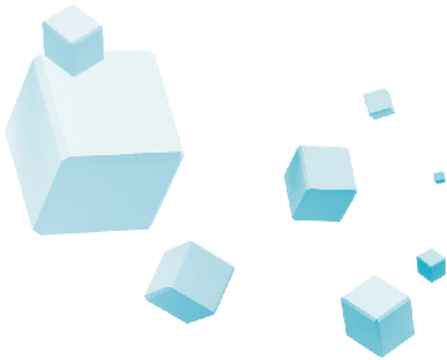
II.

암호화 종류 및 제도

제1절 암호화 종류 및 특성

제2절 안전한 암호 알고리즘

제3절 암호화 근거 법률



II. 암호화 종류 및 제도

제1절 암호화 종류 및 특성

1.1 대칭키 암호화

- 🔒 대칭키 암호화 방식은 대칭키 암호 알고리즘을 사용하여 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, LEA, HIGHT 국외의 AES, Blowfish, Camellia 등이 있다.
- 🔒 대칭키 암호화 방식의 기본 개념은 [그림 1]과 같다.

[그림 1] 대칭키 암호화 방식



1.2 공개키 암호화

- 🔒 공개키 암호화 방식은 공개키 암호 알고리즘을 사용하여 암호화하며 공개키와 개인키의 키 쌍이 존재하여 평문을 암호·복호화 하는데 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 국외의 RSA, ElGamal, ECC 등이 있다.
- 🔒 공개키 암호화 방식의 기본 개념은 [그림 2]와 같다.

[그림 2] 공개키 암호화 방식



1.3 일방향(해시함수) 암호화

- 🔒 일방향 암호화 방식은 해시함수를 이용하여 암호화된 값을 생성하며 복호화 되지 않는 방식이다.
- 🔒 해시함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해시값 또는 해시 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해시값만으로 입력 메시지를 유추할 수 없어 비밀번호와 같이 복호화 없이 입력 값의 정확성 검증이 필요한 경우 등에 사용되고 있다.
- 🔒 대표적인 해시함수로는 국외의 SHA-2(SHA-224/256/384/512), SHA-3, RIPEMD-160, Whirlpool 등이 있다.

제2절 안전한 암호 알고리즘

🔒 「개인정보의 안전성 확보조치 기준」에서는 암호화 대상 개인정보를 저장·전송시 “안전한 암호 알고리즘”으로 암호화하도록 규정하고 있으며, “안전한 암호 알고리즘”이란 국내 및 미국, 일본, 유럽 등의 해외 암호 연구 관련 기관에서 권고하는 암호 알고리즘을 의미한다.

🔒 공공기관은 국가정보원의 검증대상 암호 알고리즘을 기반으로, 민간부문(법인·단체·개인)은 국내·외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)이 권고하는 암호 알고리즘을 기반으로 「개인정보 보호법」상의 개인정보 암호화에 사용할 수 있는 안전한 암호 알고리즘의 예시는 [표 1]과 같다.

[표 1] 안전한 암호 알고리즘(예시) (2016년 9월 기준)

구분	공공기관	민간부문(법인·단체·개인)
대칭키 암호 알고리즘	SEED, LEA, HIGHT, ARIA-128/192/256	SEED ARIA-128/192/256 AES-128/192/256 Blowfish Camelia-128/192/256 MISTY1 KASUMI 등
공개키 암호 알고리즘 (메시지 암호·복호화)	RSAES-OAEP	RSA RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/256/384/512	SHA-224/256/384/512 Whirlpool 등

※ 민간부문 세부사항은 “[참고 1] 국내·외 암호 연구 관련 기관의 권고 암호 알고리즘” 참고

※ 공공기관 세부사항은 “[참고 2] 국가정보원 검증대상 암호 알고리즘 목록” 참고

🔒 권고 암호 알고리즘은 기술변화, 시간경과 등에 따라 달라질 수 있으므로, 암호화 적용 시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보를 확인하여 적용이 필요하다.

🔒 암호 알고리즘을 적용한 후에는 안전한 암호화 운영에 필요한 암호키 길이, 암호키 교환 방법, 암호 알고리즘 형태(대칭키, 공개키, 일방향)별 암호키 사용 유효기간 등 암호키 관리 관련 사항을 정하여 운영할 필요가 있다.

제3절 암호화 근거 법률

🔒 「개인정보 보호법」은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호하기 위하여 개인정보 처리에 관한 사항을 규정하고 있다.

🔒 업무를 목적으로 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 적용 대상으로 한다.

3.1 개인정보 보호법

🔒 「개인정보 보호법」에서는 고유식별정보 등 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 규정하고 있다.

📄 개인정보 보호법

- 제23조(민감정보의 처리 제한)

- ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

- 제24조(고유식별정보의 처리 제한)

- ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

- 제24조의2(주민등록번호 처리의 제한)


- ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

- 제29조(안전조치의무)

- 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.



3.2 개인정보 보호법 시행령

 법 시행령에서는 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치를 적용하도록 하고 있으며, 암호화 등 안전성 확보 조치에 관한 세부 기준은 「개인정보의 안전성 확보조치 기준」에서 정함을 명시하고 있다.



개인정보 보호법 시행령

• 제21조(고유식별정보의 안전성 확보 조치)

법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.


• 제21조의2(주민등록번호 암호화 적용 대상 등)

- ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.
- ② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.
 - 1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
 - 2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일
- ③ 행정자치부장관은 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

• 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 행정자치부장관이 정하여 고시한다.

3.3 개인정보의 안전성 확보조치 기준(행정자치부 고시)

 「개인정보의 안전성 확보조치 기준」(행정자치부 고시)에서는 고유식별정보, 비밀번호 및 바이오정보 등 암호화의 적용여부 및 적용범위 등을 규정하고 있다. 이 기준에서는 정보통신망을 통해 송신하거나 저장하는 경우 암호화 등의 안전성 확보 조치에 대한 세부 기준을 제시하고 있다.

- "고유식별정보"는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호가 여기에 해당한다.

- “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 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”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

TIP

내부망에 주민등록번호를 저장하는 경우, 「개인정보 보호법」 제24조의2, 동법 시행령 제21조의2에 따라 「개인정보의 안전성 확보조치 기준」 제7조제4항(“개인정보 영향평가”나 “암호화 미적용시 위험도 분석”)과 관계없이 암호화 하여야 한다. 이 경우에는 다음의 기간 이전까지 암호화 적용을 완료하여야 한다.

- ※ 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
- ※ 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

개인정보의 안전성 확보조치 기준 (행정자치부 고시, 제2016-35호)

• 제7조(개인정보의 암호화)

- ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
- ② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
- ③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
- ④ 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. 암호화 미적용시 위험도 분석에 따른 결과
- ⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
- ⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파괴 등에 관한 절차를 수립·시행하여야 한다.
- ⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
- ⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

부칙<제2016-35호, 2016. 9. 1.>

제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.



[표 2] 암호화 적용 기준 요약표

구분		암호화 기준	
정보통신망, 보조저장매체를 통한 송신 시	비밀번호, 바이오정보, 고유식별정보	암호화 송신	
개인정보처리 시스템에 저장 시	비밀번호	일방향(해쉬 함수) 암호화 저장	
	바이오정보	암호화 저장	
	주민등록번호	암호화 저장 ※ 2017.12.31.까지 암호화 저장: 100만명 이상 정보주체 ※ 2016.12.31.까지 암호화 저장: 100만명 미만 정보주체	
	고유식별정보 여권번호, 외국인 등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점 (DMZ)	암호화 저장
		내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부·적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보	암호화 저장 ※ 비밀번호는 일방향 암호화 저장	

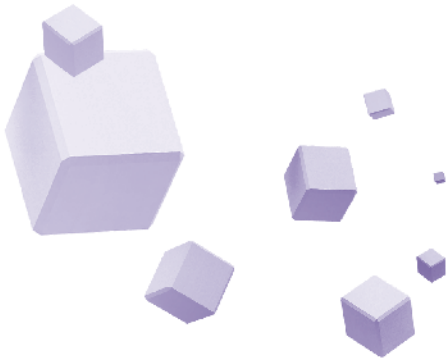
Ⅲ.

암호화 구현 및 키 관리

제1절 전송시 암호화

제2절 저장시 암호화

제3절 암호키 관리



III.

암호화 구현 및 키 관리

제1절 전송시 암호화

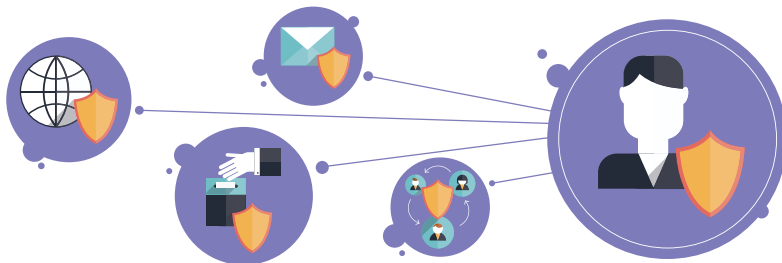
1.1 웹서버와 클라이언트 간 암호화

🔒 웹브라우저에 기본적으로 내장된 SSL/TLS 프로토콜로 접속하는 SSL 방식과 웹브라우저에 보안 프로그램을 설치하여 접속하는 응용프로그램 방식으로 구분할 수 있다.

[표 3] 웹서버와 클라이언트 간 전송시 암호화 방식 비교

방식	데이터 부분암호화	개발비용
SSL 방식	지원하지 않음	낮음
응용프로그램 방식	지원함	높음

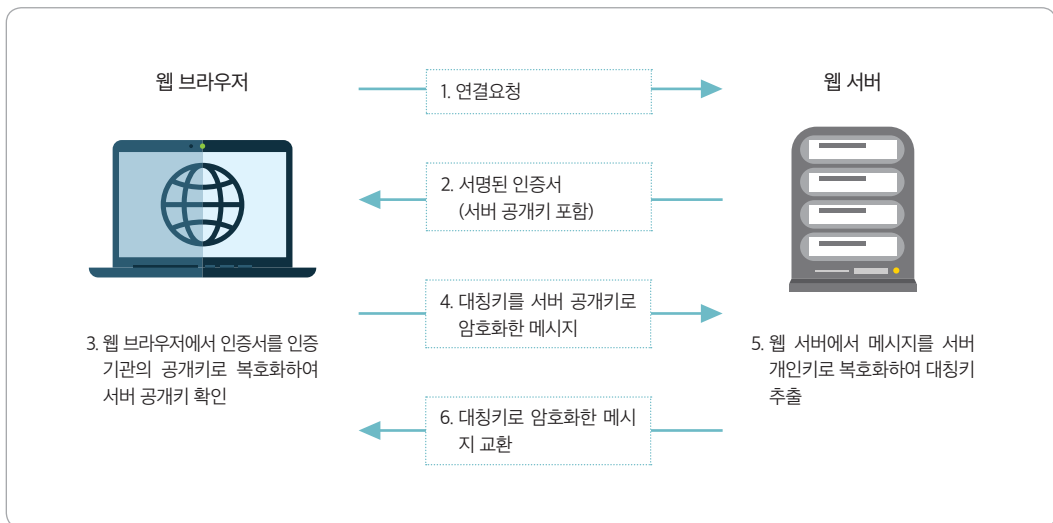
🔒 SSL 방식은 웹페이지 전체를 암호화(웹페이지 내 이미지 포함)하며 응용프로그램 방식은 특정 데이터만을 선택적으로 암호화할 수 있지만, 웹브라우저 등에 추가적인 프로그램을 설치해야 한다. 공공기관에서는 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 적용해야 한다.



1.1.1 SSL 방식

- 🔒 SSL 방식은 전송 계층(Transport Layer)을 기반으로 한 응용 계층(Application Layer)에서 암호화를 수행한다. 암호키 교환은 비대칭키 암호 알고리즘을 이용하고, 기밀성을 위한 암호화는 대칭키 암호 알고리즘을 이용하며 메시지의 무결성은 메시지 인증 코드(해시함수)를 이용하여 보장한다.
- 🔒 인터넷 쇼핑이나 인터넷 बैं킹 시 계좌정보, 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.
- 🔒 아래 그림은 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.

[그림 3] 웹서버와 웹브라우저 간의 SSL/TLS 통신 구조



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

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

1.2 개인정보처리시스템 간 암호화

- 개인정보처리시스템 간에 개인정보를 전송할 때 암호화를 지원하기 위하여 공중망을 이용한 가상사설망(VPN: Virtual Private Network)을 구축할 수 있다.
- VPN은 기반이 되는 보안 프로토콜의 종류에 따라 IPsec VPN 방식, SSL VPN 방식, SSH VPN 방식 등으로 구분할 수 있으며, 개인정보처리시스템간의 통신에서 사용할 수 있는 VPN 전송 방식의 특징을 간단히 비교하면 아래 표와 같다.

[표 4] 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

※ IPsec(IP Security Protocol) : 인터넷 프로토콜(IP) 통신 보안을 위해 패킷에 암호화 기술이 적용된 프로토콜 집합

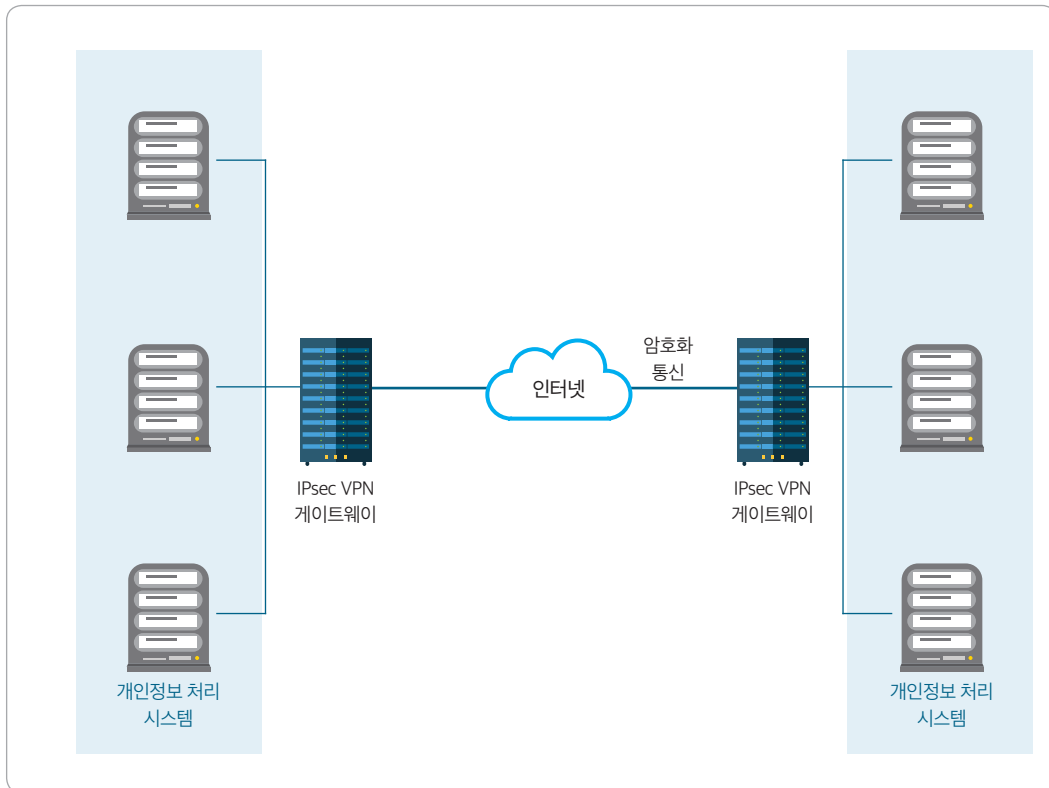
※ NAT(Network Address Translation) : 사설 IP 주소를 공인 IP 주소로 바꿔주는데 사용하는 통신망의 주소변환기

- 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 패키트의 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 있는 방식이다.
- 🔒 아래 그림은 게이트웨이 대 게이트웨이 IPsec VPN 방식을 이용하여 인터넷 구간에서 암호화 통신을 보여준다.

[그림 4] IPsec VPN 방식(게이트웨이 대 게이트웨이)의 개념도

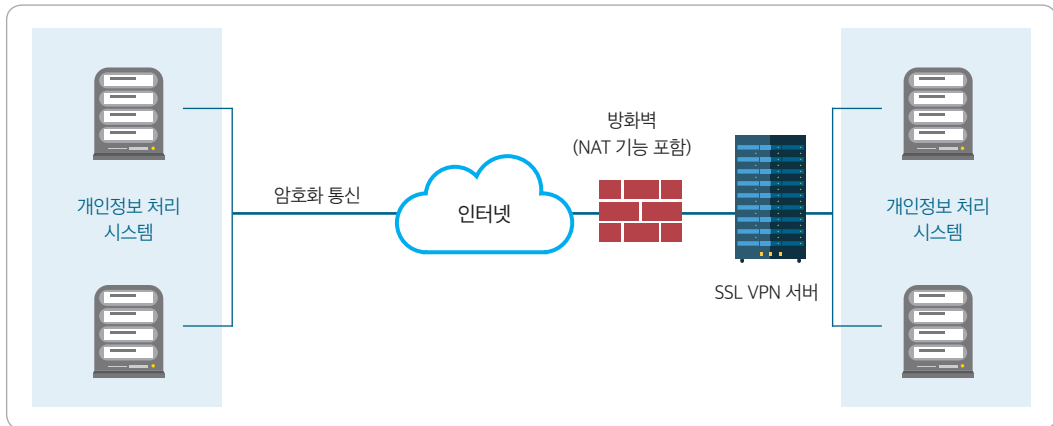


1.2.2 SSL VPN 방식

🔒 SSL VPN 방식은 응용프로그램 수준에서 SSL/TLS를 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.

🔒 아래 그림은 SSL VPN 방식에서 SSL VPN 서버를 거친 개인정보처리시스템간 암호화 통신을 보여준다. 이러한 구조는 외부망의 개인정보처리시스템과 내부의 SSL VPN 서버간 인터넷을 통한 통신에서 암호화 통신을 제공한다. 방화벽 후단의 SSL VPN 서버 없이 내부망의 개인정보처리시스템에 SSL VPN 기능을 구현하여 외부망의 개인정보처리시스템과 암호화 통신을 제공할 수도 있다.

[그림 5] SSL VPN 방식의 개념도

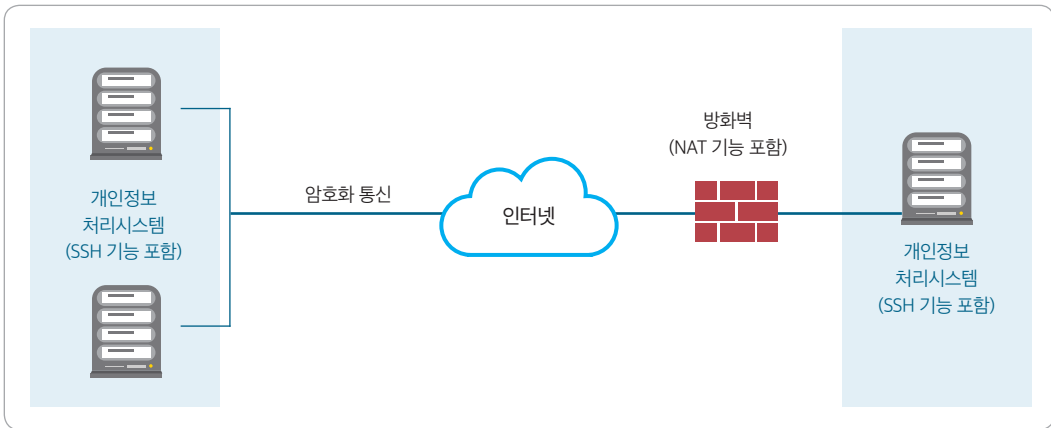


1.2.3. SSH VPN 방식

🔒 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.

🔒 아래 그림은 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 사용하여 암호화에 상응하는 보안성을 제공할 수도 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.

TIP

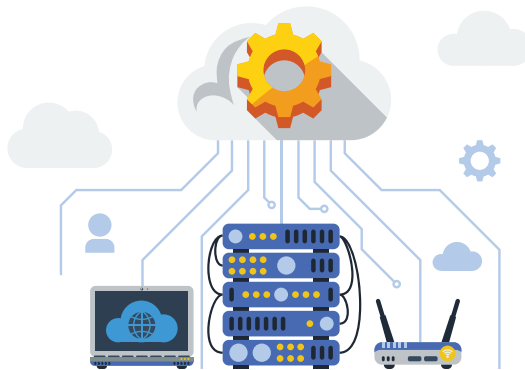
이메일을 사용하지 않고 개인정보취급자의 송·수신 컴퓨터에 VPN 기능을 구현하고 이를 통해 개인정보를 암호화하여 전송할 수도 있다.

🔒 개인정보취급자 간에 이메일을 전송할 때 사용되는 암호화 방식의 특징은 아래 표와 같다.

[표 5] 개인정보취급자 간 전송시 암호화 방식 비교

방식		공인인증서 필요 여부	표준형식
이메일 암호화	PGP	필요하지 않음	PGP 자체정의
	S/MIME	필요함	X509, PKCS#7
이메일 첨부문서 암호화		필요하지 않음	없음

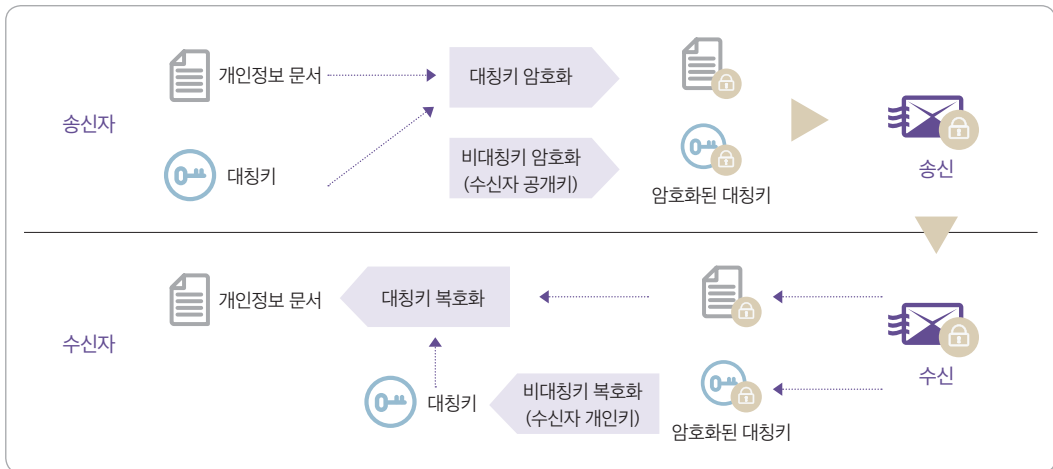
🔒 S/MIME은 공개키를 포함한 공인인증서를 발급받고 등록해야 하는 번거로움이 있다. 이에 비해 PGP의 경우 개인 간의 신뢰를 바탕으로 공개키를 등록하거나 안전한 채널로 미리 확보하는 방법을 사용할 수 있다.



1.3.1 이메일 암호화 방식

🔒 이메일 암호화 방식은 송·수신되는 이메일의 내용을 암호화함으로써 메일에 포함된 중요 개인정보의 유출을 방지하는 것이며, 대표적인 이메일 보안 프로토콜로 PGP와 S/MIME이 있다. 아래 그림은 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 공인 인증서가 있어야 한다.


1.3.2 이메일 첨부문서 암호화 방식

- 🔒 업무용 컴퓨터에서 주로 사용하는 문서 도구(예: 한글, MS 워드 등)의 자체 암호화 방식, 암호 유틸리티를 이용한 암호화 방식 등을 통해 암호화한 파일을 이메일의 첨부문서로 송·수신할 수 있다.
- 🔒 이메일을 송·수신할 개인정보취급자 간에는 미리 공유된 암호키(또는 비밀번호)를 사용하여 복호화 하며, 이 암호키는 안전하게 공유하여야 한다.

제2절 저장시 암호화

2.1 개인정보처리시스템 암호화 방식


 개인정보를 처리하고 관리하는 개인정보처리시스템은 DB에 저장된 개인정보를 암호화하여 저장함으로써 개인정보의 유출, 위·변조, 훼손 등을 방지해야 한다.


 개인정보처리시스템의 DB를 암호화할 수 있는 방식은 암호·복호화 모듈의 위치와 암호·복호화 모듈의 요청 위치의 조합에 따라 다음과 같이 구분할 수 있다.

[표 6] 모듈·위치별 암호화 방식

암호화 방식	암·복호화 모듈 위치	암·복호화 요청 위치	설 명
응용 프로그램 자체 암호화	어플리케이션 서버	응용 프로그램	<ul style="list-style-type: none"> - 암호·복호화 모듈이 API라이브러리 형태로 각 어플리케이션 서버에 설치되고, 응용프로그램에서 해당 암호·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	응용 프로그램	<ul style="list-style-type: none"> - 암호·복호화 모듈이 DB 서버에 설치되고 DB 서버에서 암호·복호화 모듈을 호출하는 방식 - 구축시 응용프로그램의 수정을 최소화 할 수 있으나 DB 서버에 부하가 발생하며 DB 스키마의 추가 필요 - 기존 Plug-In 방식과 유사
DBMS 자체 암호화	DB 서버	DB 서버	<ul style="list-style-type: none"> - DB 서버의 DBMS 커널이 자체적으로 암호·복호화 기능을 수행하는 방식 - 구축시 응용프로그램 수정이 거의 없으나, DBMS에서 DB 스키마의 지정 필요 - 기존 커널 방식(TDE)과 유사
DBMS 암호화 기능 호출	DB 서버	응용 프로그램	<ul style="list-style-type: none"> - 응용프로그램에서 DB 서버의 DBMS 커널이 제공하는 암호·복호화 API를 호출하는 방식 - 구축시 암호·복호화 API를 사용하는 응용프로그램의 수정이 필요 - 기존 커널 방식(DBMS 함수 호출)과 유사


운영체제 암호화	파일 서버	운영체제 (OS)	<ul style="list-style-type: none"> - 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 구축시 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. 아래 표는 개인정보처리시스템 암호화 방식의 선택 시 고려해야 할 사항이다.


[표 7] 암호화 방식 선택 시 고려사항

분류	고려사항
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 적용해야 한다.

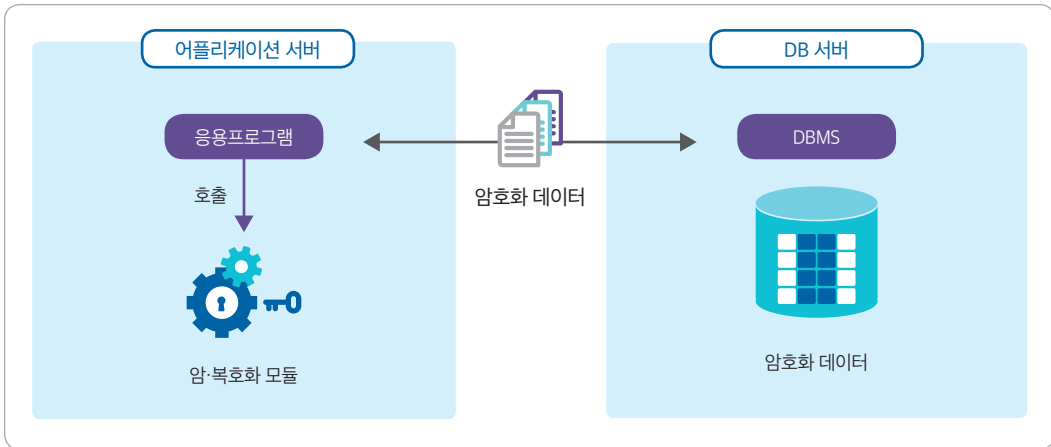
 현재 운영 중이거나 향후 개발 예정인 개인정보처리시스템의 목적 및 환경에 맞게 쉽게 구현이 가능한 암호화 방식을 선택해야 한다. 응용프로그램 및 DB 스키마 수정 등을 최소화하고 개발 환경에 맞게 성능을 최대화할 수 있도록 해야 한다.

 DB 암호화의 안전성을 확보하기 위해서는 안전한 암호키의 관리가 필요하다. 암호화된 개인정보가 유출되더라도 복호화 할 수 없도록 암호키에 대한 추가적인 보안과 제한된 관리자만 허용하도록 하는 기술을 적용해야 한다.

2.1.1 응용프로그램 자체 암호화 방식

- 응용프로그램 자체 암호화 방식은 암호·복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고 응용프로그램에서 암호·복호화 모듈을 호출하는 방식이다.
- DB 서버에는 영향을 주지 않지만 어플리케이션 서버에 암호·복호화를 위한 추가적인 부하가 발생하며, 구축 시 응용프로그램 전체 또는 일부 수정이 필요하다. 추가적으로 어플리케이션 서버와 DB 서버 간의 통신에서 암호화된 개인 정보의 전송을 보장할 수 있다.

[그림 8] 응용프로그램의 암호화 개념도



- 응용프로그램 자체 암호화 방식의 주요 특성은 아래와 같다.

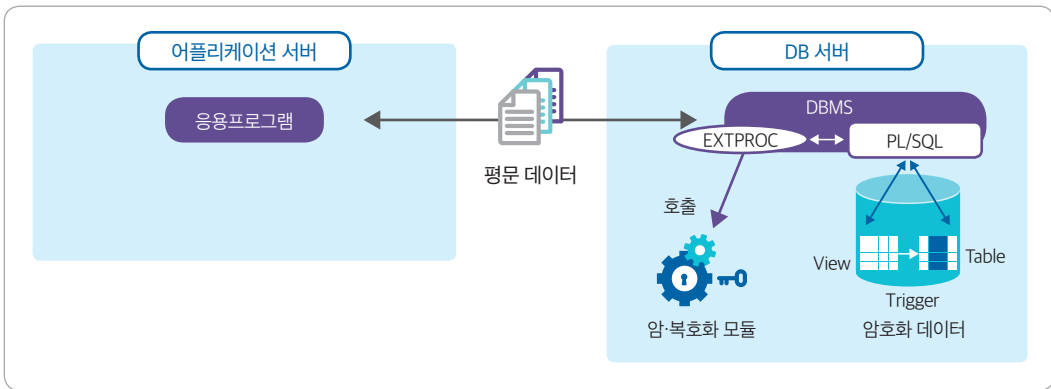
[표 8] 응용프로그램 자체 암호화 특성

분류	특성
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)

2.1.2 DB 서버 암호화 방식

- 🔒 DB 서버 암호화 방식은 [그림 9]와 같이 암호·복호화 모듈이 DB 서버에 설치되고 DBMS에서 플러그인(plug-in)으로 연결된 암호·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 암호·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 아래와 같다.

[표 9] DB 서버 암호화 방식의 주요 특성

분류	특성
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 느낄 수 있음)
응용프로그램 수정	기본적으로 수정 없이 적용할 수 있으나, 제약사항 또는 성능 문제가 있는 경우수정이 필요함
DB 스키마 수정	필요함

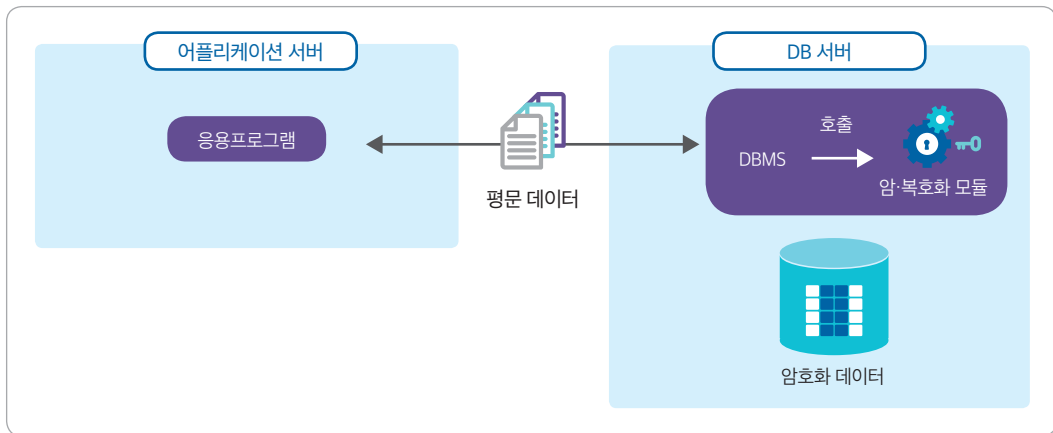
TIP

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

2.1.3 DBMS 자체 암호화 방식

- DBMS 자체 암호화 방식은 [그림 10]과 같이 DBMS에 내장되어 있는 암호화 기능(TDE : Transparent Data Encryption)을 이용하여 암호·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 아래와 같다.

[표 10] DBMS 자체 암호화 방식의 주요 특성

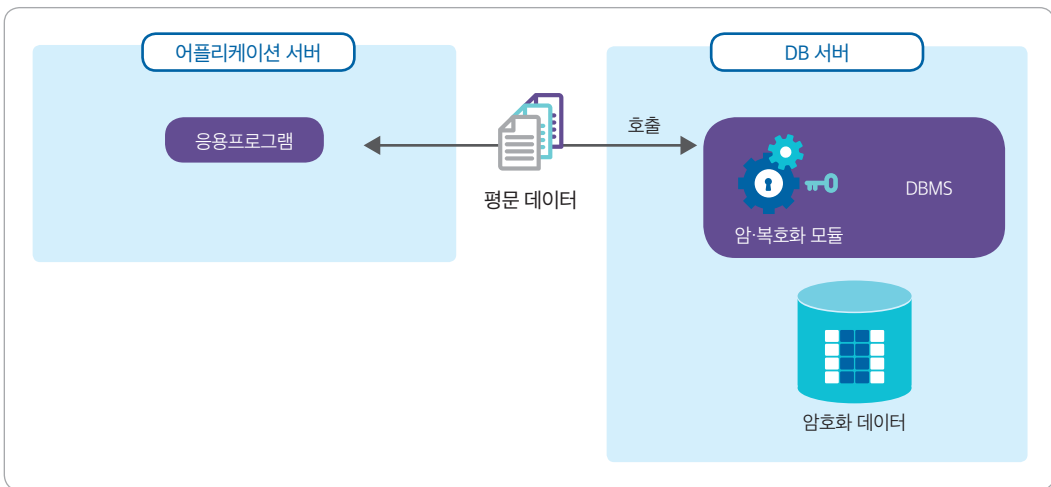
분류	특성
암·복호화 모듈	DB 서버
암·복호화 요청	DBMS 엔진
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능
응용프로그램 수정	필요하지 않음
DB 스키마 수정	거의 필요하지 않음(암호화할 DB 스키마 지정 필요)

2.1.4 DBMS 암호화 기능 호출 방식

🔒 DBMS 암호화 기능 호출 방식은 [그림 11]과 같이 DBMS가 자체적으로 암호·복호화 기능을 수행하는 API를 제공하고 해당 함수를 사용하기 위해 응용프로그램에서 호출하는 방식이다.

🔒 암호·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 아래와 같다.

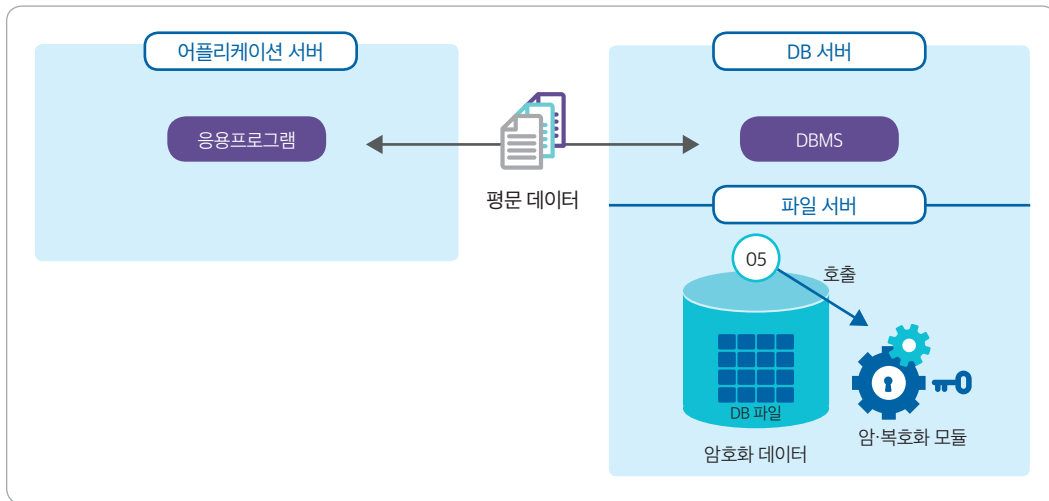
[표 11] DBMS 암호화 기능 호출 방식의 주요 특성

분류	특성
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

2.1.5 운영체제 암호화 방식

- 🔒 운영체제 암호화 방식은 [그림 12]와 같이 OS에서 발생하는 입출력 시스템 호출을 이용한 암·복호화 방식으로 DB 파일 자체를 암호화한다.
- 🔒 응용프로그램이나 DB 스키마의 수정이 필요하지 않지만 DB 파일 전체를 암호화 하는데 따른 파일 서버 및 DB 서버에 추가적인 부하가 발생할 수 있다.

[그림 12] 운영체제 암호화 방식의 개념도






- 🔒 운영체제 암호화 방식의 주요 특성은 아래와 같다.

[표 12] 운영체제 암호화 방식의 주요 특성

분류	특성
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·보조저장매체 암호화 방식

- 
 업무용 컴퓨터에서는 하드디스크, 이동식 디스크 또는 보조저장매체(USB 등)에 저장된 개인정보의 보호를 위해 개별 문서 파일 단위 암호화, 디렉터리 단위 암호화, 디스크 암호화 등의 방법을 사용할 수 있다.
- 
 파일 암호화는 업무용 컴퓨터의 하드디스크, 이동식 디스크, 보조저장매체에 저장된 개인정보에 대한 보호뿐만 아니라 개인정보취급자 간에 네트워크상으로 파일을 안전하게 전송하기 위한 방식으로도 사용할 수 있다.
- 
 업무용 컴퓨터에서 하드디스크, 이동식 디스크, 보조저장매체에 적용 가능한 암호화 방식은 [표 13]과 같이 구분할 수 있다.

[표 13] 업무용 컴퓨터 암호화 방식의 구분

분류	특성
문서 도구 자체 암호화	<ul style="list-style-type: none"> • 업무용 컴퓨터에서 사용하는 문서도구의 자체 암호화 기능을 통하여 개인정보 파일 암호화
암호 유틸리티를 이용한 암호화	<ul style="list-style-type: none"> • 업무용 컴퓨터의 OS에서 제공하는 파일 암호 유틸리티 또는 파일 암호 전용 유틸리티를 이용한 개인정보 파일, 디렉토리의 암호화
DRM (Digital Right Management)	<ul style="list-style-type: none"> • DRM을 이용하여 다양한 종류의 파일 및 개인정보 파일의 암호화 • 암호화 파일의 안전한 외부 전송이 가능함
디스크 암호화	<ul style="list-style-type: none"> • 디스크에 데이터를 기록할 때 자동으로 암호화하고, 읽을때 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 14]와 같다.


[표 14] 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: 한글, MS 워드 등)로 작성한 파일

** 일반문서 : 특정 문서 이외의 문서(예: 텍스트 파일, 이미지 파일 등)


2.2.1 문서 도구 자체 암호화 방식


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


2.2.2 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.

2.2.3 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.

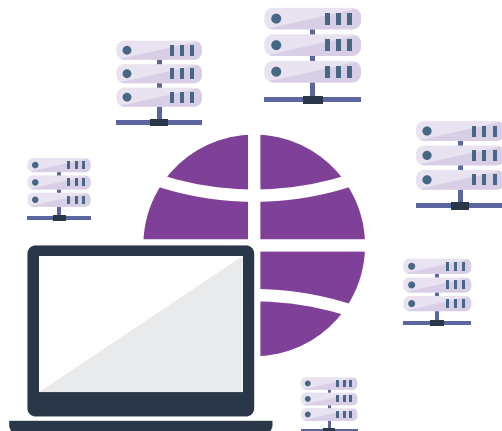
 DRM으로 암호화된 문서는 DRM 클라이언트가 없는 PC에서는 열람이 불가능하며, 열람 중에도 파일이 복호화 되지 않고 암호화 상태를 유지한다. 또한, 암호화 파일의 안전한 외부 전송이 가능하다.

2.2.4 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.

2.2.5 기타 암호화

- 🔒 기타 하드웨어 또는 소프트웨어적인 암호화 도구나 방식 등을 사용하여 암호화를 수행할 수 있다. 다만, 이 경우에는 안전한 암호 알고리즘을 사용하는지, 해당 기관에 적용되는 규정·지침 등에 적합한지 등을 확인하여 적용이 필요하다.



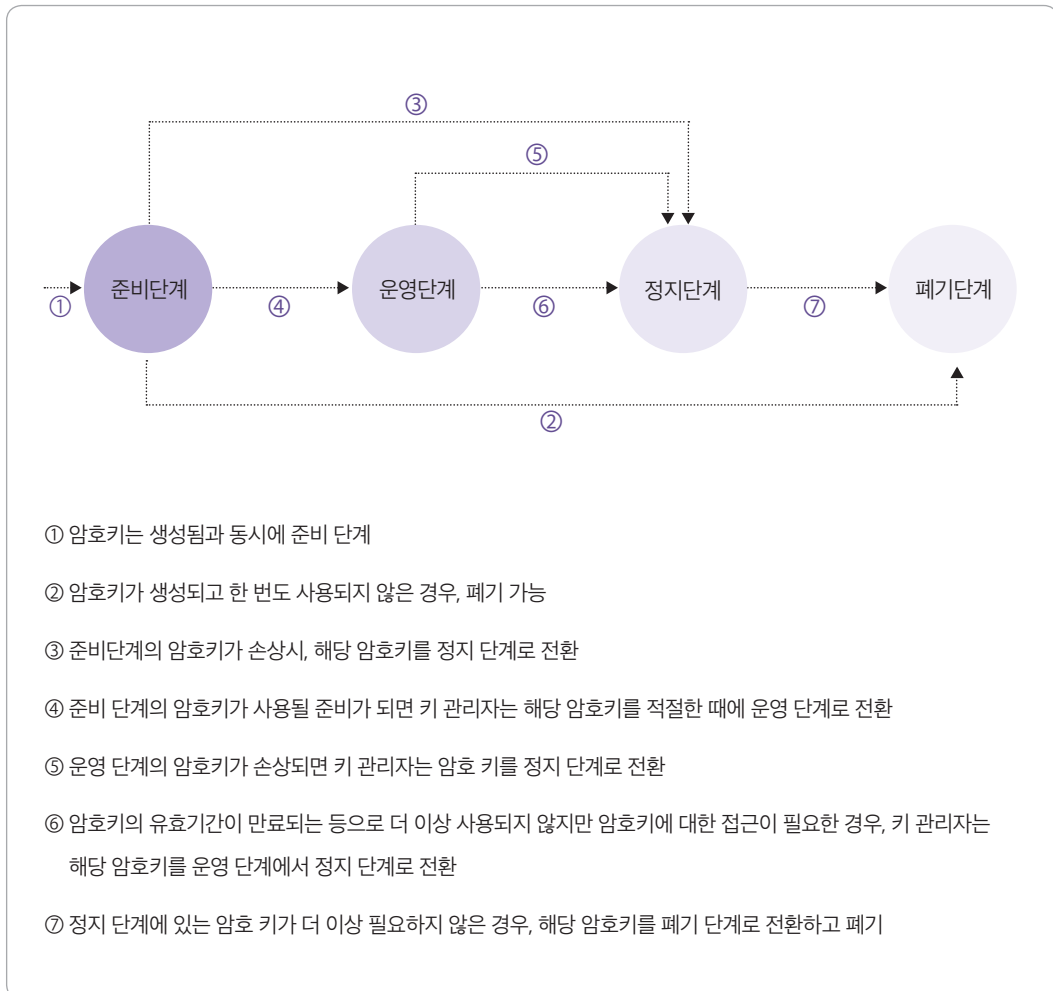
제3절 암호키 관리

3.1 암호키 수명주기

🔒 암호키 관리시의 상태와 기능에 따라 키 수명주기는 아래와 같이 나눌 수 있다.


- 준비 단계 : 암호 키가 사용되기 이전의 단계이다.(미생성 또는 준비 상태)
- 운영 단계 : 암호 키가 암호 알고리즘 및 연산에 사용되는 단계이다.(운영 상태)
- 정지 단계 : 암호 키가 더 이상 사용되지 않지만, 암호 키에 대한 접근은 가능한 단계이다.(정지 또는 위험 상태)
- 폐기 단계 : 암호 키가 더 이상 사용될 수 없는 단계이다.(폐기 또는 사고 상태)

[그림 13] 암호키 수명주기



3.2 단계별 암호키 관리

3.2.1 준비 단계

 준비 단계에서는 암호키를 사용할 사용자나 암호키가 사용될 시스템을 설정한다. 사용자 등록 기능, 시스템 초기화 기능, 사용자 초기화 기능, 키 자료 설치 기능, 키 설정 기능, 키 등록 기능 등이 해당한다.

암호키 생성

- 난수발생기(RBG) 이용
 - 암호키 생성에 필요한 난수는 안전한 난수발생기(RBG)를 이용하여 생성하도록 한다. 난수발생기에 대한 구체적인 개요와 요구사항에 대해서는 KS X ISO IEC 18031을 참고할 수 있으며, 이를 준수해야 한다.
- 비대칭키 알고리즘의 키 생성
 - 디지털 서명을 위한 키 쌍 생성 : 디지털 서명 알고리즘에서 사용하는 키 쌍의 생성에 대해서는 KS X ISO IEC 14888-3을 참고할 수 있으며, 난수발생기에서 계산된 난수를 디지털 서명 알고리즘의 키 쌍을 생성하는데 필요한 난수로 사용해야 한다.
 - 키 설정을 위한 키 쌍 생성 : 키 설정은 하나 또는 그 이상의 실체가 공유 비밀 키를 사용할 수 있도록 하는 절차를 의미하며 키 합의(실체들 간에 공유 비밀 키를 설정)와 키 전송(보호되는 암호 키를 한 실체에서 다른 실체로 전송)을 포함한다.
- 대칭키 알고리즘의 키 생성
 - 미리 공유된 키를 이용한 키 유도 : 난수발생기를 이용하여 생성될 수도 있고, 키 합의 구조를 이용하여 생성될 수도 있으며, 키 유도 함수와 미리 공유된 다른 키를 이용하여 생성될 수도 있다. TTKA, KO-12,0241을 참고할 수 있다.
 - 패스워드를 이용한 키 유도 : 패스워드를 선택할 때 높은 엔트로피를 가지는 패스워드를 선택할 것을 권장하며, PKCS #5를 참고할 수 있다.
 - 다수의 암호 키를 이용한 키 생성 : n개의 암호키 K_1, \dots, K_n 이용하여 암호 키를 생성하거나 이러한 암호 키와 독립적인 m개의 정보 V_1, \dots, V_m 을 이용하여 암호 키를 생성할 수 있다. 여기서 K_1, \dots, K_n 은 공개되지 않아야 하며, V_1, \dots, V_m 은 공개되어도 된다.

암호키 분배

- 대칭키 알고리즘의 키 분배
 - 수동적 키 분배 : 비밀키나 개인키를 수동적으로 분배할 때, 암호키들은 암호화 되어 분배되거나 물리적으로 안전한 절차에 의해 분배되어야 한다.
 - 자동화된 키 전송 : 통신 채널(예시: 인터넷·위성 전송)을 이용하여 암호 키를 분배하는데 사용된다.

- 비대칭키 알고리즘의 키 분배
 - 대칭키 알고리즘의 키를 분배하는 방법과 동일한 방법으로 개인키를 분배하여 개인키에 대한 무결성과 기밀성을 보장한다.
- 기타 키 자료 생성 및 분배
 - 영역 파라미터, IV(Initial Value), 공유된 비밀, RNG 시드, 다른 공개 및 비밀정보, 중간 값, 난수, 비밀번호 등이 있다.

3.2.2 운영 단계

암호키 저장

- 암호키는 암호키에 대한 유효기간이 만료되기 전까지 운영 상태에 있다. 암호키의 유효기간동안 사용되는 키 자료들은 필요에 따라 장비 모듈에 보관되거나 저장 매체에 보관 된다.

암호키 가용

- 암호키의 유효기간 동안 하드웨어 손상 또는 소프트웨어 오류 등의 사유로 암호키는 항상 손상될 가능성이 있으므로 가용성 보장을 위해서는 키 백업 및 키 복구 기술이 필요하다.


암호키 변경

- 암호키의 변경은 운영중인 암호 키를 다른 암호키로 교체하는 것을 의미한다. 암호키가 노출된 경우, 노출의 위험이 있는 경우, 암호키의 유효기간의 만료가 가까워지는 경우에는 키를 안전하게 변경해야 한다. 암호키 변경은 키 교체, 키 갱신 함수, 키 유도 함수 등이 있다.


3.2.3 정지 단계

보관과 키 복구


- 키 자료의 보관은 무결성과 접근통제가 가능해야 한다. 보관된 정보는 수정이 불가능한 상태이거나 새로운 보관 키를 이용하여 주기적으로 암호화 되어야 한다. 또한, 보관된 정보는 운영 데이터와 분리되어 보관되어야 하며, 암호 정보의 사본들은 물리적으로 분리된 곳에 보관되어야 한다. 보관 키로 암호화되는 중요한 정보에 대한 보관키는 백업되어야 하며, 사본은 다른곳에 보관되어야 한다.
- 키 자료의 복구는 보관되어있는 다른 정보를 복호화 하거나 인증할 때 필요하다. 키 복구에 필요한 암호 연산을 수행하기 위하여 보관 장소로부터 원하는 키 자료를 회수하거나 재생성하여 키 복구를 수행한다.

 실체 말소


- 보안 도메인에 속해있는 실체의 권한을 삭제한다. 말소된 실체의 키 자료의 사용을 방지하기 위한 것이다.

 키 말소

- 더 이상 키 자료가 필요하지 않거나 관련된 정보가 유효하지 않을 경우, 키 자료는 키 자료와 관련된 모든 기록들과 함께 키 자료가 더 이상 사용되지 않음을 나타내는 표시를 통해 말소된다. 일반적으로 키를 등록된 제3의 기관에서 수행한다.


 키 파기


- 암호키의 사본을 만들 때, 이에대한 관리는 최종 파기를 위해 필요하다. 모든 개인키나 대칭키의 복사본이 더 이상 필요하지 않다면 즉시 파기되어야 한다.

 키 취소

- 키 손상, 기관으로부터 실체의 삭제 등의 이유로 정상적인 유효기간의 중간에 키 자료를 제거하는 경우 필요하다. 키 취소는 키 자료를 더 이상 사용할 수 없음을 나타낸다.

3.2.4 폐기 단계

-  폐기 단계에서는 키 자료를 더 이상 사용할 수 없다. 일반적으로 폐기 단계의 키 자료에 대한 모든 기록은 이미 삭제되어 있어야 한다. 그러나 일부 단체에서는 감사를 목적으로 특정 키 속성 유지가 필요할 수도 있다.

-  폐기 상태의 암호키와 사고 상태의 암호키들의 특성에 대한 기록을 유지함으로써 수명주기 동안 손상된 키를 추적할 수 있다. 손상된 키로 저장한 정보는 정보 자체가 손상될 수 있다.



3.3 암호키 유효기간

🔒 암호키 유효기간은 사용자 또는 관리자가 암호키를 사용할 수 있는 기간 또는 특정 시스템에 주어진 암호키의 유효성이 유지되는 기간이다.

3.3.1 암호방식별 키 유효기간

🔒 비대칭키의 유효기간 : 비대칭 암호화 방식의 개인키와 공개키 각각은 키 유효기간을 가지고 있다. 키의 유효기간은 인증서의 유효기간과 동일할 필요는 없으며, 새로운 인증서 발급시 유효기간도 그만큼 연장된다.

🔒 대칭키의 사용기간 및 유효기간 : 대칭 암호화 방식은 암호 복호화에 사용하는 키가 동일하다. 대칭키에 대한 유효기간은 발신자 사용기간이 시작할 때부터 수신자 사용기간이 끝날 때 까지이다.

3.3.2 키 유형별 유효기간 설정 시 고려사항

🔒 키 유형은 암호키를 사용하는 환경이나 정보만큼 암호키의 유효기간에 영향을 준다.

[표 15] 키 유형에 따라 권장하는 키 유효기간

키 유형	키 유효기간		키 유형	키 유효기간	
	발신자	수신자		발신자	발신자
개인 서명키	1~3년		공개키 전송키	1~2년	
공개 서명 검증키	키 크기에 따라 다름		대칭키 합의키		
개인 인증키	1~2년		개인 고정키 합의키		
공개 인증키			공개 고정키 합의키		
대칭 인증키	2년이하	(발신자기간+3년) 이하	개인 임시키 합의키	하나의 키 합의 트랜잭션	
대칭 암호키			공개 임시키 합의키		
대칭키 암호키			대칭 인가키		
대칭/공개 RNG키	리시딩에 따라 다름		개인 인가키	2년이하	
대칭 마스터키	약 1년		공개 인가키		
개인키 전송키	2년이하				

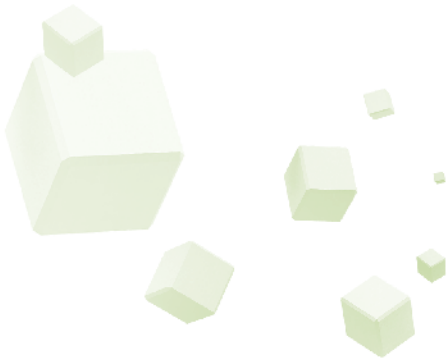
IV.

암호화 추진 절차 및 사례

제1절 암호화 추진 절차


제2절 전송시 암호화 사례

제3절 저장시 암호화 사례



IV.

암호화 추진 절차 및 사례

 본 장에서는 개인정보처리시스템의 암호화 추진 절차 및 다양한 암호화 방식별 적용 사례를 제시한다.

주의사항

- 본 장에서 제시되는 절차 및 사례는 단순 참고용으로 아래 제시된 각 사례에서 암호화 관련 처리속도, 소요기간, 투입인력, 처리량 등은 특정 환경에서 수행된 사례로 대부분의 일반적인 환경에 적용되지 않음
- 또한 본 장에서 제시되는 절차 및 사례는 간략한 이해 목적으로 처리속도, 소요기간, 투입인력, 처리량 등에 영향을 미칠 수 있는 다양한 세부 사항들은 생략하였음
- 따라서, 암호화를 적용하는 해당 개인정보처리자는 자신의 환경에 맞추어 암호화 추진절차에 따라 세부적인 분석 후 적용 필요

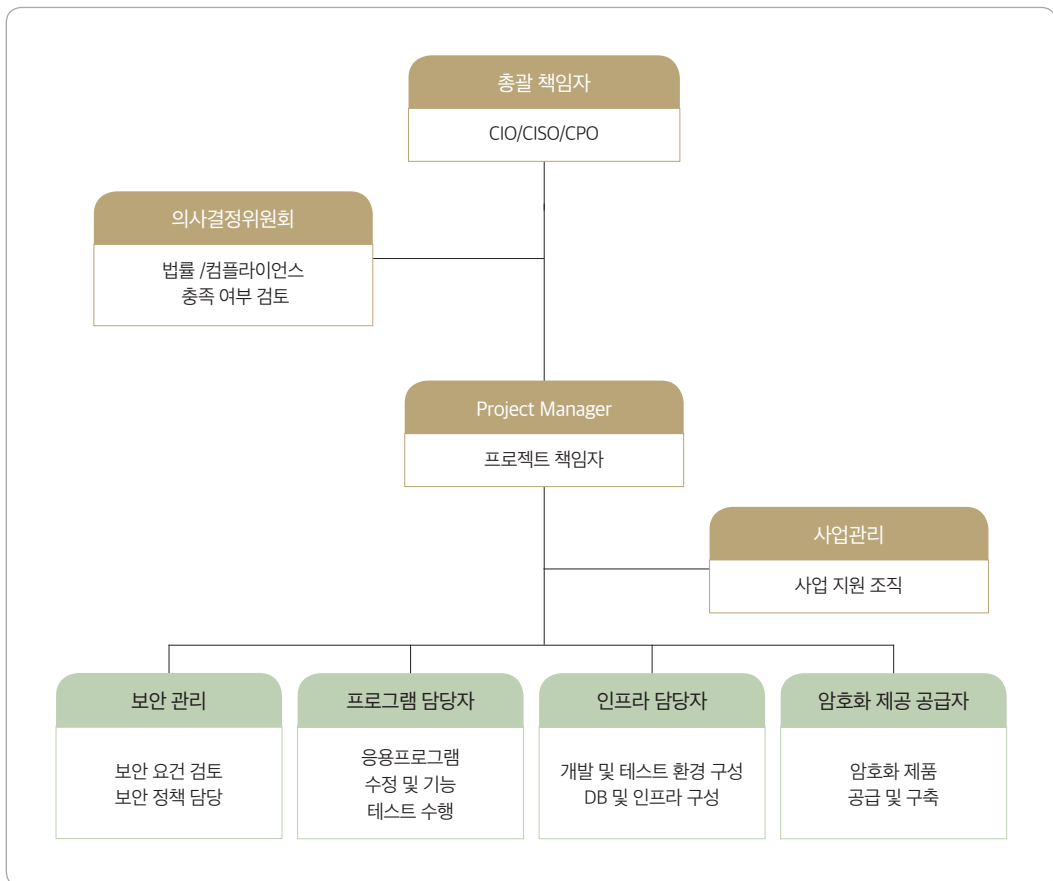
제1절 암호화 추진 절차


1.1 암호화 계획 수립

1.1.1 암호화 수행 조직 구성

- 🔒 암호화 수행은 보안, DBMS, 응용프로그램, 인프라 등 다양한 조직의 협업이 필수적 이므로 암호화 수행 조직과 조직별 역할을 정확히 정의하고 원활한 사업 수행을 위한 협업 방안을 수립해야 한다. 다음은 암호화 구축을 위한 조직 체계와 각 조직별 역할과 책임 예시이다.


[그림 14] 암호화 수행 조직도(예시)



 암호화 수행 조직의 역할과 책임은 다음과 같다.


[표 16] 암호화 수행 조직의 역할 및 책임(예시)

구분	역할 및 책임
총괄 책임자	<ul style="list-style-type: none"> • 암호화 등 개인정보 보호관련 계획 수립 및 이행, 감독 등 총괄 개인정보처리자
의사결정 위원회	<ul style="list-style-type: none"> • 법률 검토, 위험관리 등 의사결정
프로젝트책임자(PM)	<ul style="list-style-type: none"> • 프로젝트 관리 총괄 • 암호화 적용 정책 관리 <ul style="list-style-type: none"> - 암호화 적용 대상(주민등록번호, 비밀번호 등) - 암호 알고리즘(SEED, ARIA, AES 등) - 적용 정책(일방향 암호화, 부분암호화 등) - 적용 방식(API, Plug-In 등) • 암호키 관리
사업관리 담당자	<ul style="list-style-type: none"> • 프로젝트 진행 관리 <ul style="list-style-type: none"> - 범위, 비용, 위험/이슈, 품질, 의사소통 등 관리
보안관리	<ul style="list-style-type: none"> • 법률 및 보안성 검토, 보안 정책 수립 및 운영 등
응용프로그램 담당자	<ul style="list-style-type: none"> • 응용프로그램 내 개인정보 사용 부분 추출 • 암호화 적용 프로그램 결과 검증 • 암호화 적용 소스 배포 및 형상 관리 • 운영시스템 내 개인정보 암호화 적용
인프라 담당자	<ul style="list-style-type: none"> • DBMS 또는 파일 내 개인정보 사용 부분 추출 • 솔루션 설치 지원 • 개발 및 테스트 환경 구성 및 지원
암호화 제품 공급자	<ul style="list-style-type: none"> • 솔루션을 이용한 암호화 적용 가이드 • 암호화 이행 지원

 암호화 적용을 위한 소요 인력 규모를 검토한다.


- 사업 수행 인력 공수
 - 기관 내부 인력 소요 공수
 - 외부 기관/업체 위탁 시 필요 공수

1.1.2 운영 환경 분석


 법/규정에서 의무적으로 암호화 하도록 지정한 대상과 보안성 강화를 위해 추가적으로 암호화를 수행할 대상 등을 정의한다.

[표 17] 개인정보 보호법 암호화 적용 대상

암호화 대상	비고
주민등록번호 외국인등록번호 여권번호 운전면허번호 바이오정보 비밀번호	<ul style="list-style-type: none"> • 바이오정보 : 지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보 • 비밀번호 : 일방향 해쉬함수 적용

 개인정보 보유 현황 및 개인정보처리시스템 운영 환경 등을 파악한다.

- 개인정보 보유 현황 분석
 - 개인정보 저장 유형 분석(DBMS, File 등)
 - 개인정보파일명, DBMS명, 테이블, 컬럼, 사이즈, 보유 건수 등 현황 분석
- 개인정보처리시스템 운영 환경 분석
 - 개인정보처리시스템의 개발언어, 서비스 방식(WEB, C/S, Batch 등), 관련(수정 대상) 프로그램 분수 등 현황 분석
 - CPU, Memory, Storage 등 자원 가용 및 할당율 확인을 통한 증설 여부 등 검토
- 개인정보처리시스템 내·외부 연계 현황 분석
 - 개인정보 처리 유형(배포, 수집, 이용) 분석
 - 암호화에 따른 시스템 간 영향도 분석
- 개인정보처리시스템 리소스 분석
 - CPU, Memory, Storage 등 현재 사용 중인 자원 사용률을 분석하여 증설 필요 여부 검토

 암호화 적용 대상 개인정보를 삭제나 대체 또는 변경 가능 여부를 검토하여 암호화 대상을 확정한다.

1.1.3 암호화 적용 방식 검토

 개인정보 암호화를 위해 암호화 방식별 특징과 장·단점 등을 사전 검토한다.

[표 18] 암호화 방식 및 장·단점 비교

구분	방식	특징	장점	단점
컬럼 암호화	API	응용프로그램 소스를 수정 (암·복호화 함수 적용)하여 암·복호화 수행	<ul style="list-style-type: none"> • 암·복호화 속도가 빠름 • 암·복호화 과정이 WAS의 응용프로그램에서 수행되므로 DBMS 부하 분산 효과 • 암호화 구간이 길다 	<ul style="list-style-type: none"> • 응용프로그램 변경에 따른 개발 비용 발생 • 적용된 미들웨어의 패치에 영향을 받을 수 있음
	Plug-In	DBMS내 Plug-In 형태 모듈을 적용하여 암·복호화 수행	<ul style="list-style-type: none"> • 응용프로그램 변경 최소화 (암·복호화 View 사용 제약 SQL, 성능 제약 SQL 수정 필요) 	<ul style="list-style-type: none"> • DBMS 서버의 자원을 사용하여 대용량 처리 시 DB서버에 부하 발생 가능 • 암호화 구간이 짧음 • DBMS 패치에 따라 영향을 받을 수 있음
	Hybrid	API방식과 Plug-In 방식을 조합하여 사용	<ul style="list-style-type: none"> • 응용프로그램 변경 최소화와 부하 분산 효과를 얻을 수 있음 	<ul style="list-style-type: none"> • API 적용 부분의 응용프로그램 변경에 따른 개발 비용 발생
	Token	암호화된 데이터와 Token 형태의 치환 값을 사용	<ul style="list-style-type: none"> • 암호화 후 컬럼이나 변수의 길이 변경이 없기 때문에 I/F 관련 응용프로그램의 변경이 필요 없음(API 방식과 비교하여 상대적으로 응용 프로그램 변경 비율이 낮음) 	<ul style="list-style-type: none"> • 암호화 적용 데이터 타입 제한
	TDE	DBMS Kernel Level에서 암·복호화 수행	<ul style="list-style-type: none"> • 암·복호화 속도가 Plug-In보다 상대적으로 빠름 • 기존 응용 프로그램의 수정 불필요 	<ul style="list-style-type: none"> • 데이터에 접근 권한을 가진 사용자에게 모두 복호화 되어 보여짐 • 일부 DBMS만 지원(Oracle, MS-SQL, Tiberio 등) • 국가기관 미 인증 (인증여부 별도 확인 필요)
블록 암호화	File	OS의 Kernel Level에서 File에 대해 암·복호화 수행	<ul style="list-style-type: none"> • 기존 응용프로그램의 수정 불필요 	<ul style="list-style-type: none"> • 암호화 구간이 매우 짧음


※ 암호화 방식은 운영체제 패치에 따라 영향을 받을 수 있음

 시스템 규모에 따라 주로 사용되는 암호화 방식은 다음과 같다.


[표 17] 암호화 적용 방식(예시)

구분	특성 및 고려 사항	암호화 적용 방식
시스템 규모	소형	Plug-In, File, TDE 등
	중형	API, Hybrid, TDE, File 등
	대형	API, Hybrid, File 등
서비스 유형	OLTP 유형	API, Hybrid, TDE, File 등
	OLAP, Batch 유형	API, TDE, File 등
암호화 적용 관점	성능 우선 고려	API 등
	저비용 우선 고려	Plug-In 등
응용프로그램 수정 난이도	난이도 상	API, Plug-In 등
	난이도 중 / 하	Plug-In, TDE, File 등
보안성 관점	데이터의 암호화 유지 구간	API 등
기타	구조 변경이 어려운 경우	Token 등

1.1.4 소요 기간 및 비용 산정

 시스템 현황 분석 및 암호화 적용 방식 등을 고려하여 예상되는 암호화 소요 기간을 산정한다.

- 개인정보 보유량, 연계 시스템, 응용프로그램, 시스템 규모 등을 고려하여 암호화 적용 방식에 따른 소요 기간 산정

 상용 암호화 솔루션 도입하기 위해서는 솔루션 도입을 위한 라이선스 비용과 암호화 솔루션 운영을 위한 H/W 및 S/W 도입 비용을 검토한다.

- 라이선스 비용 산정을 위해서는 암호화 대상 업무 시스템의 CPU(또는 Core 수), DBMS 종류, 이중화 구성 여부, 개발, 검증, DR 구성 여부 등의 현황 정보의 파악이 필요할 수 있다.
- 암호화 솔루션 운영을 위한 H/W와 WAS, DBMS등의 SW가 필요할 수 있다.
- 기관에서 사용하고 있는 보안솔루션, 백업솔루션 등과 연계가 필요한 경우 Agent 도입 비용 등을 포함하여야 한다.

1.1.5 암호화 업체 선정

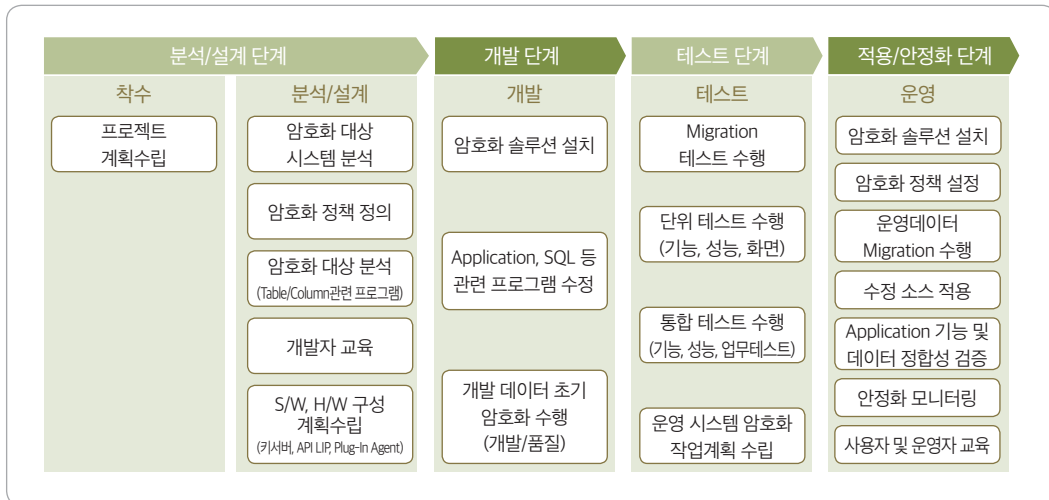
🔒 개인정보 암호화를 수행하기 위해서는 다양한 고려 사항과 암호화 솔루션 및 관련 기술이 필요하다. 자체적으로 암호화 수행 가능한 기술력을 보유한 경우를 제외하고는 일반적으로 암호화 업체를 선정하여 사업을 수행하며 이를 위한 사업자 선정에 위한 절차는 다음과 같다.

- 정보제공요청서(Request For Information) 의뢰
 - 사업의 개략적인 계획을 기술하여 공급업체에게 사업계획 검토와 세부 실행을 위한 정보 제공을 요청
- 제안요청서(Request For Proposal) 작성
 - 사업 수행에 필요한 요구사항을 제시하여 공급업체에게 공식적인 제안을 요청
- 사업 공고 및 제안서 접수
 - 요구사항을 충족하기 위한 제안 업체의 사업 수행 방안을 검토
- BMT 수행
 - 하드웨어 및 소프트웨어의 성능을 측정
- 사업자 선정
 - 사업 수행에 적합한 사업자를 선정

1.2 암호화 수행

🔒 암호화 수행은 분석·설계 단계, 개발 단계, 테스트 단계, 적용·안정화 단계로 분류하며 아래의 그림과 같다.

[그림 15] 암호화 수행 프로세스(예시)



1.2.1 분석·설계 단계

- 암호화 대상 시스템 분석
 - 시스템 환경(OS, CPU, Memory, DISK, DB 등) 및 접속 정보 확인
 - 키관리 서버 및 Agent 사용 Port 오픈 요청
- 암호화 정책 정의
 - 암호화 대상 시스템 정의
 - 암호화 대상 정보 정의
 - 암호화 정책(부분암호화 적용 여부, 암호 알고리즘 등) 정의
 - 암호화 방식(API, Plug-In(UDF Only 포함), Hybrid 등) 정의
 - 접근제어, 감사로그 적용 대상 정의
- 암호화 대상 테이블·컬럼 및 프로그램 분석
 - 미사용 또는 불필요한 개인정보 삭제 가능 여부 검토
 - 암호화 대상 테이블·컬럼 파악
 - 암호화 대상 테이블·컬럼을 이용하는 응용프로그램의 SQL 구문 및 소스 도출
 - Batch, Function, Procedure, crontab Job 등 확인
 - 타 업무 시스템(내부·외부) 간 Interface 확인(EAI, DB Link, FTP 연계 등)
- 개발자 교육
 - 암호화 대상 테이블·컬럼에 대한 응용프로그램 개발 또는 수정에 필요한 함수 사용 방법 교육
- 키관리 서버 구성 계획 수립
 - H/W도입 시 설치 일정, Network, 전원 등 관련 계획 수립

1.2.2 개발 단계

- 암호화 솔루션 설치
 - 키관리 서버 설치
 - 개발 환경에 암호화 솔루션 설치
- 응용프로그램 수정
 - 암호화 대상 테이블·컬럼을 이용하는 응용프로그램 SQL 수정(Plug-In 방식 적용 시 성능 또는 기능상 필요 SQL에 대해 구문 수정)
 - Batch, Function, Procedure 수정
 - 타 업무 시스템(내부/외부) 간 Interface 응용프로그램 확인 및 SQL 수정
 - 단방향암호화(패스워드)적용대상 응용프로그램 절차수정(패스워드 생성, 로그인, 패스워드 수정, 패스워드 찾기 등)

- 개발 데이터 초기 암호화 수행(개발/품질)
 - 불필요 보유 개인정보 및 임시 생성 데이터 삭제
 - 암호화 대상 Table의 여유 용량 확인
 - 개발 시스템 데이터를 대상으로 초기 암호화 수행(초기 암호화 수행 시간 확인, DBMS 객체 확인)

1.2.3 테스트 단계


- Migration 테스트 수행
 - 대량 데이터 이행 시 소요 시간 측정
 - History 데이터, Log 등 사전 암호화 가능 데이터 초기 암호화 및 이행 소요 시간 측정
- 단위 테스트 수행
 - 단위 SQL 및 메뉴 등에 대한 성능 및 기능 측정(암호화 쿼리별 응답 속도 측정, 암호화 전·후 응용프로그램 성능 테스트, SQL 튜닝 등)
- 통합테스트 수행
 - 응용프로그램 통합 테스트(메뉴 및 응용프로그램간 통합 기능 테스트 및 Online, Batch, I/F, Report 등 전체 Process 통합 테스트 수행)
- 이중화 테스트 수행
 - 키관리 서버 및 암호복호화 적용 서버의 이중화 테스트
- 운영 암호화 작업 계획 수립
 - 작업 시간 및 인력 계획
 - Batch, Backup, 외부 Interface 중지를 위한 사전 준비(작업공지, 유관 부서 협조 등)

1.2.4 적용·안정화 단계


- 암호화 솔루션 설치
 - 운영시스템에 암호화 모듈 설치(Plug In, API Module 등)
- 암호화 정책 설정
 - 암호화 대상, 암호화 알고리즘, 부문 암호화 적용 여부 등 정책 등록
- 운영데이터 초기 암호화 수행
 - 암호화 대상 테이블·컬럼 암호화 진행
 - 초기 데이터 암호화
 - 암호화 대상 테이블(Table)의 제약조건 정상 상속 여부 확인


- 수정 소스 적용
 - 응용프로그램, SQL, Batch, Function, Procedure 등의 수정사항 반영
- 응용프로그램 기능 및 데이터 정합성 검증
 - 응용프로그램 성능 및 기능 테스트
 - 암호화 전·후 데이터 정합성 및 DBMS Object 검증
- 안정화 모니터링
 - 암호화 적용 후 시스템 자원(CPU, Memory등) 및 응용프로그램(SQL) 성능 및 암호화 솔루션 모니터링
- 사용자 및 운영자 교육
 - 암호화 대상 추가·변경·제거 등 DBMS 운영 관련 교육
 - 암호화 솔루션 운영 교육

1.3 암호화 수행시 고려사항


 개인정보 암호화로 개인정보처리시스템의 중요한 데이터 형태가 변경되므로 응용프로그램, DBMS, 인터페이스, 시스템, 인프라, 보안 등 전반적인 영향도를 고려하여야 하며, 이에 따라 각각의 부분을 담당하고 있는 운영 및 관리 조직 간의 긴밀한 협업이 필수적인 사항이라 할 수 있다. 다음은 암호화 적용 시 주요 고려 사항이다.


- 예를 들어, API 암호화 방식으로 암호화를 적용하는 경우 암호화 대상 개인정보를 포함하고 있는 테이블·컬럼을 모두 식별해야 하며, 응용프로그램 내부에서 대상 컬럼을 사용하는 정확한 위치를 확인해야만 해당 부분의 수정 및 테스트가 가능하며 데이터 암호화 적용 이후의 안전성을 확보 할 수 있다.
- 암호화 대상 업무 시스템과 기관 내부의 타 시스템 간 연계되어 있는 인터페이스와 대외 기관과의 인터페이스 부분을 정확히 식별해야 한다. 외부로 암호화가 적용된 데이터를 보내는 경우 암호키 공유 등의 문제로 평문으로 전환하여 보내야 하는 경우가 대부분이며, 기관 내부 업무 시스템들은 암호화된 데이터를 복호화 없이 사용할 수 있도록 구성할 수 있으므로, 타 시스템과의 인터페이스(In·Out) 지점에서 암·복호화 적용 여부를 판단해야 한다.
- 암호화 적용 시 추가로 필요할 수 있는 시스템 자원을 분석하여 필요 시 자원의 사전 확보가 필요하다.
 - 저장 공간: 암호화 후 데이터 길이 증가, 암호화 작업용 임시 공간, 암호화 관련 로그 데이터(감사로그, 작업 이력) 저장 공간 등을 고려하여 여유 공간을 확보해야 한다.
 - CPU/Memory 사용률: 암·복호화 연산 수행으로 CPU 및 Memory 사용률이 증가할 수 있다.

 불필요하거나 과도한 개인정보를 보유하는 경우 개인정보 관리를 위한 비용과 암호화 적용을 위한 시간 및 비용이 과다 소요되므로, 개인정보 암호화의 기본 전제는 불필요하게 보유하고 있는 개인정보의 안전한 폐기라 할 수 있다. 또한 주민등록번호를 대체할 수 있는 방안도 함께 검토되어야 한다.


 데이터 암호화를 적용하면 일반적으로 암호화 전보다 응답 속도 지연이나 시스템 사용을 증가 등 성능이 저하 될 수 있으며, 암·복호화 처리 절차를 최적화함으로써 이를 최소화 할 수 있다.

- Inner Join 등의 작업 시 불필요한 복호화 절차 제거
- Batch 처리 시 불필요한 복호화 제거
- 부분 암호화 적용을 통한 복호화 절차 제거
- SQL 튜닝, 업무 프로세스 개선을 통한 성능 개선

 일반적으로 Plug-In 방식(암·복호화 View Trigger를 이용하여 자동으로 암·복호화를 수행) 적용 시 성능 저하 가능성이 있으며, View Trigger를 이용하여 자동으로 수행 되는 암·복호화 부분에 대해 불필요한 암·복호화를 수행하지 않도록 구성하면 암·복호화 성능을 개선할 수 있다.


 운영 시스템에 암호화를 적용하는 작업 수행 시 사전 준비, 암호화 이행, 이행 후 검증, 안정화 등의 작업 절차를 거치며 각 단계별 작업 사항에 대한 충분한 준비와 검토가 필요하다.

- 작업 절차 정의 시 고려 사항
 - 사전 준비 사항 확인
 - 암호화 이행 절차 및 소요 시간 분석
 - 이행 후 검증 방안 수립
 - 백업 및 원복 방안 확보
- 작업 담당자별 주요 역할과 책임 정의
 - 의사결정 담당: 암호화 작업 진행 총괄 및 오픈, 원복 등의 주요 의사 결정
 - 인프라 담당: 응용프로그램 백업, DBMS 백업, WAS 구동 등 인프라 관련 작업 수행
 - 암호화 작업 담당: 암호화 이행 및 검증
 - 응용프로그램 담당: 응용프로그램 소스 배포, 암호화 후 응용프로그램의 정상 동작 확인

 암호화를 적용하게 되면 관리 프로세스, 데이터 형태, 응용프로그램 개발과 사용 시 기존 환경에서 변화되는 부분에 대한 고려가 필요하다.


- 관리 프로세스 변경 및 추가
 - 암호화 대상 및 정책 관리
 - 암호화 기관리


- 암·복호화 데이터에 대한 접근 및 사용 권한 관리
- 암호화 관련 로그 관리

 컬럼 암호화 적용 시 데이터 길이 및 순서 등이 변경되므로 응용프로그램 개발 및 사용 시 이에 대한 고려가 필요하다.


- 응용프로그램 개발 부분의 암호화 데이터 사용 유무
- 데이터 사용 프로세스 변경(저장 시 암호화, 사용 시 복호화)
- 데이터 길이 변경으로 인한 변수 길이 고려
- 데이터 순서 변경으로 조건 검색 방식 변경

1.3.1 대규모 개인정보 암호화 수행 시 고려사항

 암호화 적용 시 기 보유 중인 평문 데이터에 대해 일괄 암호화를 적용하는 시간이 필요하며 통상 데이터 정합성 확보를 위해 시스템을 중지하고 작업을 수행하는데, 대용량 데이터 암호화 이행 시 암호화 이행만 수십 시간에서 수일이 소요 될 수 있으므로 관공서 등에서는 시스템 작업을 위해 업무를 중지할 수 있는 시간이 제한적인 경우 초기 암호화 이행에 필요한 시간에 대한 방안을 수립하여야 한다.

 자원 사용률 증가

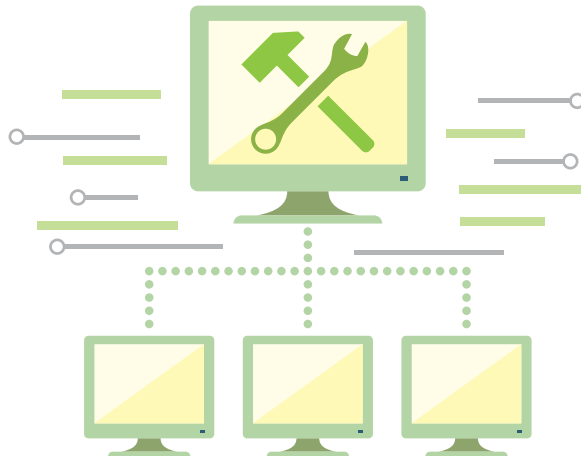
- 암호화된 데이터는 평문보다 길이가 늘어나게 된다. 따라서 데이터 길이 증가로 인한 디스크 사용량이 증가되며 개발시스템, 검증시스템, 운영시스템, DR시스템, 백업시스템 등에 대해 저장 및 사용 공간의 증가가 필요하며 디스크, 스토리지와 관련 장비, 라이선스 등의 증설이 필요할 수 있다.
- 암·복호화 처리를 위해 연산을 수행하므로 CPU 및 Memory 사용률이 일부 증가할 수 있다.

 응용프로그램 변화로 인한 영향도

- 암·복호화 처리를 위해 암호화(저장·수정) 부분, 복호화(조회) 부분의 정확한 식별과 소스 수정이 필요하며, 평문 대비 길이가 길어지는 암호화된 데이터의 처리를 위한 변수 사이즈 조정이 필요할 수 있다. (응용프로그램 내부 변수, 인터페이스 연계 프로토콜 내 해당 부분 사이즈 등)
- 패키지 시스템, 프레임워크, 인터페이스 연계 솔루션, 레포팅 툴 등 기관내부에서 개발된 시스템 이외 도입된 솔루션의 수정 가능 여부의 검토가 필요하다.
- 암호화 적용 작업 시 업무 시스템의 정상 동작을 위한 검증을 수행하여야 하며, 대용량 암호화 이행 시 암호화 이행뿐만 아니라 데이터 정합성 확인, 응용프로그램 정상 동작 검증 등을 위한 작업 시간 확보와 검증 절차 및 수행방법의 수립이 필요하다.

1.3.2 소규모 개인정보 암호화 수행 시 고려 사항

- 1. 기존 구축된 시스템에 대해 저비용, 단기간 암호화를 적용하기 위해서는 File(Kernel) 암호화 방식이나 Plug-In(암·복호화 View) 적용 등 소스 수정이 불필요하거나 최소화 할 수 있는 암호화 방식의 도입을 검토하여 적용할 수 있다. File(Kernel) 암호화 방식은 패키지 시스템처럼 제조사의 지원 없이 응용프로그램의 소스 수정이 불가능한 경우에도 암호화를 적용할 수 있다.
- 2. 신규로 시스템 구축하거나 패키지 시스템을 도입하는 경우 개인정보 암호화를 고려하여 개발하고 패키지 도입 시 개인정보 암호화가 적용된 제품을 우선 고려하는 것도 방안이 될 수 있다.
- 3. 한글·워드·엑셀 등 문서 작성 프로그램을 이용하여 사용자가 PC에 생성, 저장하여 사용하는 경우 개인정보의 보호를 위해 프로그램에서 제공하는 저장 암호를 사용하거나 PC 파일 암호화 솔루션 등을 이용하여 파일 암호화를 적용 한다.
- 4. PC 내 개인정보를 검색하여 사용자에게 알려주는 솔루션 등을 통해 불필요하게 보유하고 있는 개인 정보를 폐기하도록 유도하는 방안도 고려할 수 있다.

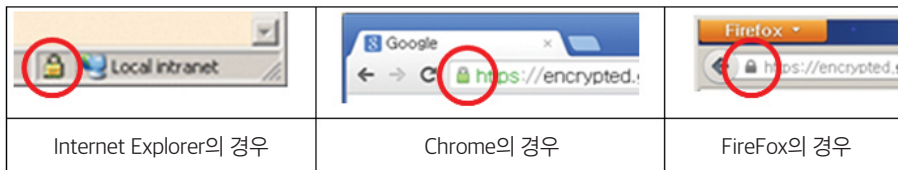


제2절 전송시 암호화 사례

2.1 웹서버와 클라이언트 간 암호화 (아파치(Apache) 웹서버 이용)

- 🔒 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 16]과 같이 웹브라우저 주소창 또는 하단의 상태표시줄에 자물쇠 표시가 나타나게 된다.

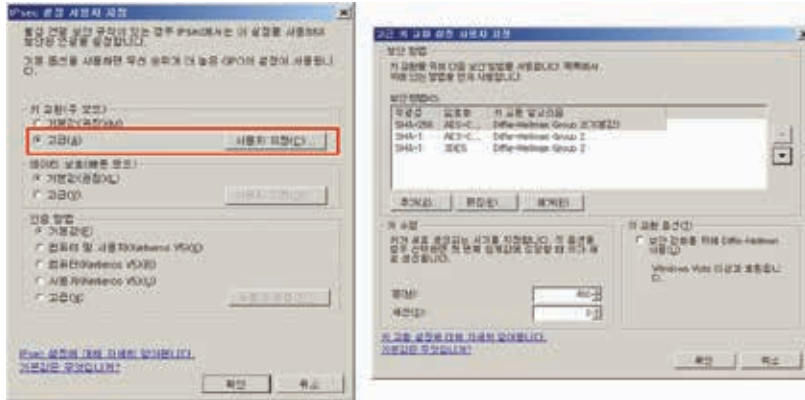
[그림 16] SSL 방식에서 나타나는 웹브라우저 자물쇠 표시



2.2 개인정보처리시스템 간 암호화 (윈도우 7에서 IPsec VPN 이용)

- 🔒 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 17]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 17] Windows 7에서 IPsec VPN 방식을 위한 암호 알고리즘 설정

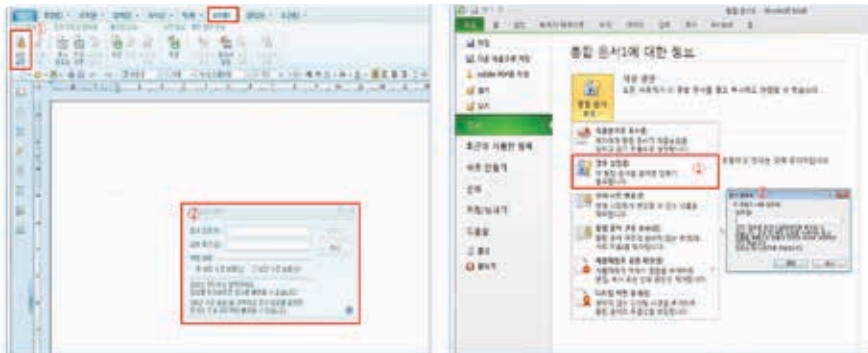


2.3 개인정보취급자 간 암호화 (이메일 첨부문서 암호화)

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

- 한글 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 18] 한글 2010과 MS 엑셀 2010에서 문서 암호화 설정



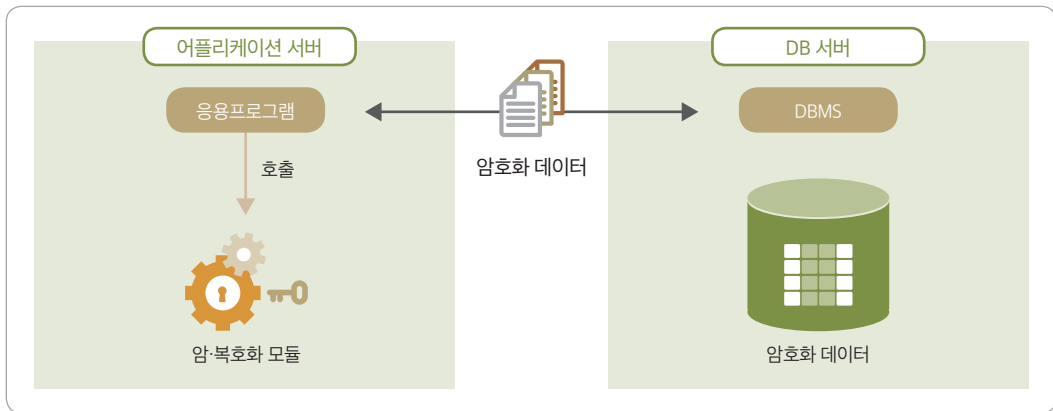
🔒 암호화된 문서를 이메일에 첨부한 후, 수신자에게 이메일을 전송한다.

제3절 저장시 암호화 사례

3.1 개인정보처리시스템 암호화

3.1.1 응용프로그램 자체 암호화 방식 (API 방식)

[그림 19] API 방식



🔒 DB서버 당 개인정보 암호 처리 사례

- 시스템 사양 : Xeon 24 Core 3.0Ghz, 32GB Memory, AIX
- 처리 데이터
 - 크기 : 13억 건 (File size 31G)
 - 내용 : 주민등록번호, 계좌번호, 거래내역 등
- 암호화 전후 주요 업무 Batch 및 온라인 응답시간 비교


[표 20] Batch 암호화 전·후 처리속도 비교

데이터량 (건)	처리속도 (초)		차이 (초)
	암호화 전	암호화 후	
50,000	10.9x	12.8x	1.8x
1,000,000	22.6x	23.3x	0.7x

- OLTP(On Line Transaction Process) 테스트

[표 21] OLTP 암호화 전·후 처리속도 비교

데이터량 (건)	처리속도 (초)		차이 (초)
	암호화 전	암호화 후	
50,000	0.006x	0.006x	0
1,000,000	0.006x	0.006x	0

 암호화 소요기간 사례

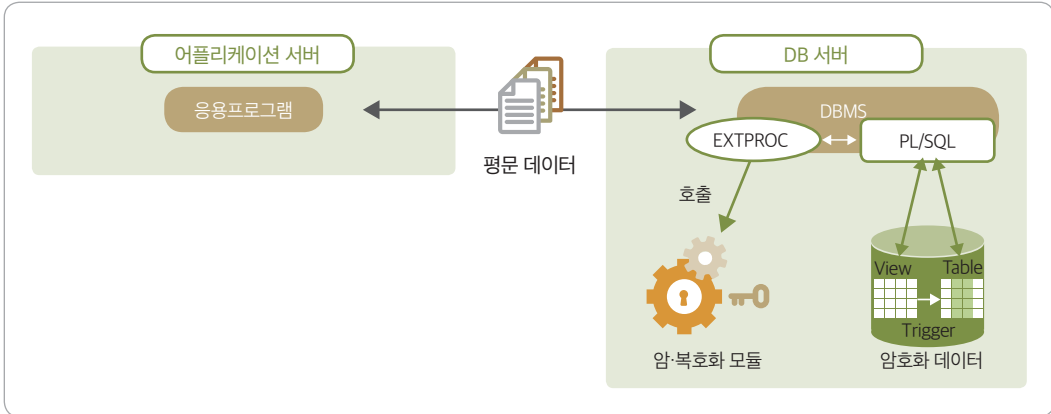
[표 22] API 방식 암호화 사례 비교

구분	A사	B사	C사	D사
주민번호 처리량	60,000건	800,000건	7,000,000건	11,000,000건
연계 시스템수	2개	5개	8개	14개
투입인력	중급 2 (9M/M)	중급 1 (2M/M)	고급 2, 중급 4, 초급 2 (39M/M)	고급 1, 중급 1 (5M/M)
소요기간	6개월	2개월	6개월	3개월



3.1.2 DB서버 암호화 방식 (Plug-in 방식)

[그림 20] Plug-in 방식



🔒 DB서버 당 개인정보 암호 처리 사례

- 시스템 사양 : Xeon Core8 2.4Ghz, 16GB Memory, AIX
- 처리 데이터
 - 크기 : 1800만 건 (File size 3.xG)
 - 내용 : 주민등록번호, 거래내역정보 등
- 암호화 전후 주요 업무 응답시간 비교

[표 23] 암호화 전·후 처리속도 비교

데이터량 (건)	처리속도 (초)		차이 (초)
	암호화 전	암호화 후	
100	0.0x	0.0x	0.0x
1,000	0.2x	0.3x	0.1x
10,000	10.9x	12.3x	1.4x

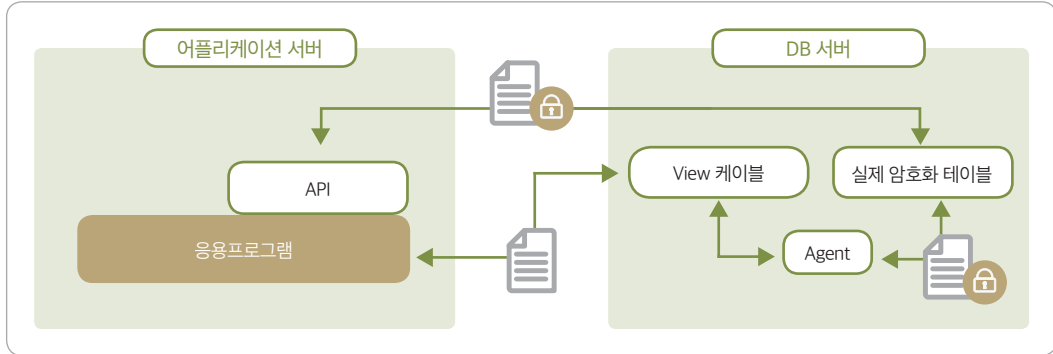
🔒 암호화 소요기간 사례

[표 24] Plug-in 방식 암호화 사례 비교

구분	A사	B사	C사	D사	E사
주민번호 처리량	800,000건	500,000건	500,000건	80,000,000건	1,360,000건
연계 시스템수	3개	3개	2개	11개	8개
투입인력	중급 1 (3M/M)	고급 1, 중급 2 (4.5M/M)	중급 1 (1M/M)	중급 2, 초급 1 (11.5 M/M)	고급 1, 중급 2 (6.5 M/M)
소요기간	3개월	2.5개월	1개월	5개월	3개월

3.1.3 응용프로그램 및 DB서버 암호화 혼용 방식 (Hybrid(API + Plug-in) 방식)

[그림 21] Hybrid(API + Plug-in) 방식



🔒 DB서버 당 개인정보 암호 처리 사례

- 시스템 사양 : Xeon 8 Core 2.9Ghz, 16GB Memory, AIX
- 처리 데이터
 - 크기 : 2억8천만 건 (File size 13G)
 - 내용 : 주민등록번호, 외국인등록번호, 여권번호 등
- 주요 업무 응답시간 테스트
 - API 부분 테스트

[표 25] API 부분 암호화 전·후 처리속도 비교

데이터량 (건)	처리속도 (초)		차이 (초)
	암호화 전	암호화 후	
50,000	0.01x	0.02x	0.00x
1,000,000	0.05x	0.05x	0.00x

- Plug-in 부분 테스트

[표 26] Plug-in 부분 암호화 전·후 처리속도 비교

데이터량 (건)	처리속도 (초)		차이 (초)
	암호화 전	암호화 후	
50,000	0.02x	0.02x	0.00x
1,000,000	0.06x	0.06x	0.00x

🔒 암호화 소요기간 사례

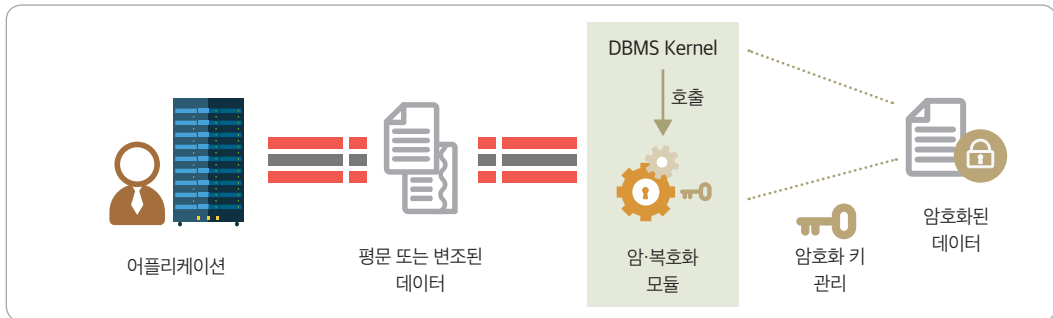
[표 27] Hybrid(API+Plug-in) 방식 암호화 전·후 처리속도 비교

구분	A사	B사	C사	D사
주민번호 처리량	900,000건	500,000건	1,100,000건	86,000,000건
연계 시스템수	4개	2개	13개	7개
투입인력	중급 2, 초급 2 (12M/M)	중급 1 (1M/M)	고급 1, 중급 1 (7.5M/M)	중급 2, 초급 3 (26M/M)
소요기간	4개월	1개월	4.5개월	8개월

3.1.4 DBMS 자체 암호화 (TDE 방식)

🔒 TDE 방식 구성

[그림 22] TDE 방식




🔒 DB서버 당 개인정보 암호 처리 사례

- 암·복호화 모듈이 DBMS Kernel 자체에 내장되는 형태이며, 대상 데이터는 디스크 상의 데이터 파일을 포함한 일체의 저장소에서 암호화된 상태로 저장됨
- 어플리케이션에는 평문 또는 적절히 변조된 데이터로 반환됨
 ※ 데이터 변조 기능은 Oracle 11gR2 11.2.0.4 버전부터 지원
 - Kernel에 내장된 기능으로 암호화 대상 데이터 크기에는 특별한 제한이 없음
- BMT/POC 사례

[표 28] TDE 방식 적용 사례

구분		암호화 후 성능변화
DB서버	CPU 사용률	OLTP 3~5% 증가 대량 데이터셋 배치 5~10% 증가 (단, H/W 가속 기능 사용 시 1~3% 증가)
	MEMORY 사용률	변화 없음
WAS서버	CPU 사용률	변화 없음
	MEMORY 사용률	변화 없음
DISK 사용량		변화 없음

 암호화 소요기간 사례

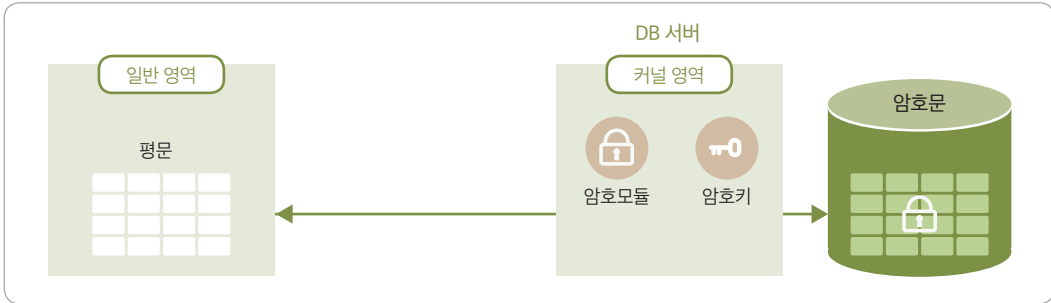
[표 29] TDE 방식 암호화 사례 비교

구분	A사	B사
암호화 대상	1TB	100GB
투입인력	특급 1M, 고급 3M(4M/M)	특급 1.5M, 고급 1.5M(3M/M)
소요기간	3개월	1.5개월



3.1.5 운영체제 암호화 방식 (File 암호화 방식)

[그림 23] File 암호화 방식



- 🔒 DB서버 당 개인정보 암호 처리 사례
 - 시스템 사양 : Core2Quad Q6600, 4GB Memory
 - 처리 데이터
 - 초기 암호화 시 분당 약 420,000건 처리 예상

- 🔒 암호화 소요기간 사례

[표 30] File 암호화 방식 암호화 사례 비교

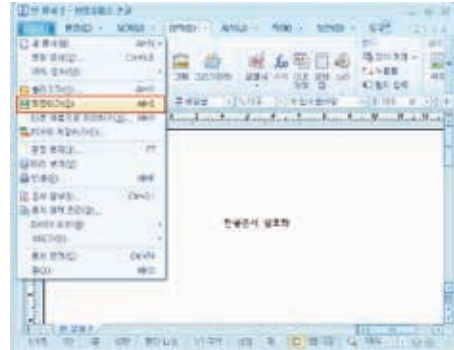
구분	A사	B사	C사
주민번호 처리량	500,000건	900,000건	13,000,000건
연계 시스템수	3개	7개	9개
투입인력	중급 1 (2M/M)	고급 1, 중급 1 (2M/M)	고급 1, 중급 1 (2M/M)
소요기간	2개월	2개월	2개월


3.2 업무용컴퓨터(보조저장매체 포함) 암호화

3.2.1 문서 도구 자체 암호화(한글)

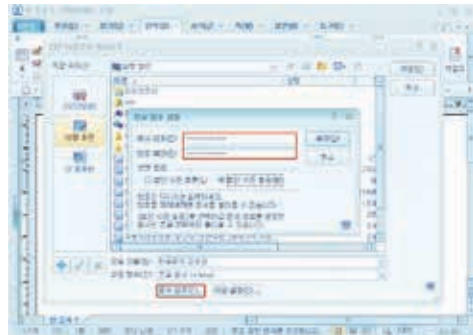
 문서를 작성하여 저장하기 메뉴를 클릭한다.


[그림 24] 한글 문서 화면



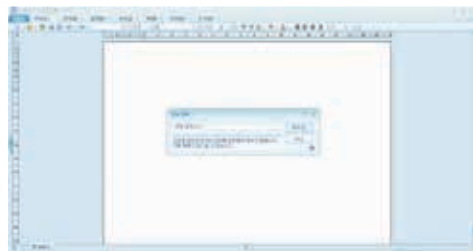
 문서암호 버튼을 눌러 해당 문서에 지정할 암호를 입력하고 설정버튼을 클릭한다.

[그림 25] 한글 문서 암호 설정 방법



 해당 문서 열기(더블 클릭)시에 암호가 설정된 것을 확인할 수 있다

[그림 26] 한글 문서 암호 적용된 화면

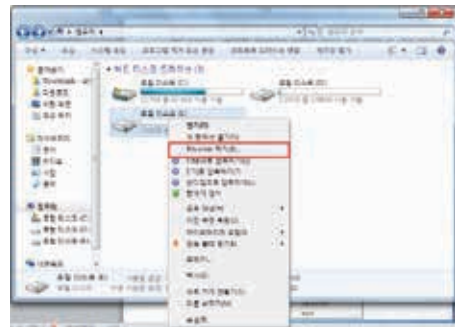


3.2.2 암호 유틸리티를 이용한 암호화 (윈도우 BitLocker로 보조저장매체 암호화)

Windows OS 제공하는 BitLocker 기술이 있으며, 현재 Windows Vista, Windows 7, Windows 8, Windows 10 등에서 BitLocker를 지원하고 있다.

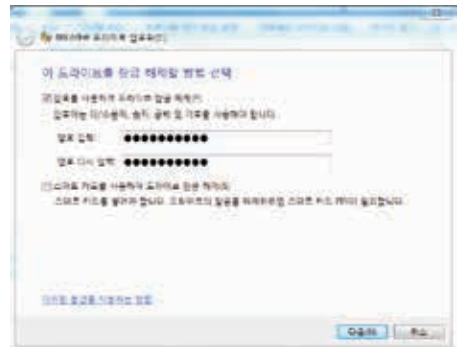
먼저 암호화할 보조저장매체에 BitLocker를 실행시킨다.
 ※ 보조저장매체가 아닌 특정 디렉토리를 선택하여 암호화도 가능

[그림 27] 보조저장매체 BitLocker 실행 화면



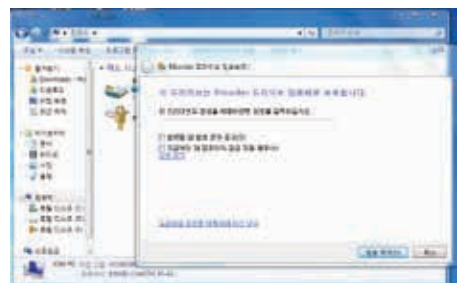
[그림 28] 보조저장매체 암호 설정 방법

보조저장매체의 드라이브 잠금 해제 암호를 입력한 후 암호화를 수행한다.



[그림 29] 보조저장매체 암호 적용된 화면

암호화 완료 후 보조저장매체를 실행(더블클릭)하면 암호화를 확인할 수 있으며, 드라이브 잠금 해제 암호를 입력하면 암호화를 풀어 내용을 확인 할 수 있다.

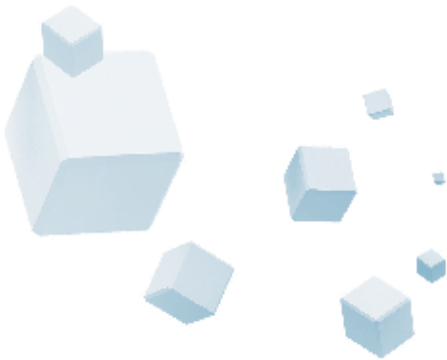


V.

부록

[제1절 FAQ](#)

[제2절 참고자료](#)



IV. 부 록

제1절 FAQ

[Q1]. 개인정보 보호법 상의 암호화 대상은 무엇이며 어떻게 암호화해야 하나요?

개인정보 보호법상 암호화 대상은 고유식별정보(주민등록번호, 외국인등록번호, 운전면허번호, 여권번호), 비밀번호, 바이오정보입니다. 암호화 대상 정보를 전송시 그리고 저장시 아래 표에 따라 암호화하여야 합니다.

[암호화 적용 기준 요약표]

구 분		암호화 기준	
정보통신망, 보조저장매체를 통한 송신 시	비밀번호, 바이오정보, 고유식별정보	암호화 송신	
개인정보처리시스템에 저장 시	비밀번호	일방향 암호화 저장	
	바이오정보	암호화 저장	
	고유식별정보	주민등록번호	암호화 저장 ※ 2017.12.31.까지 암호화 저장: 100만명 이상 정보주체 ※ 2016.12.31.까지 암호화 저장: 100만명 미만 정보주체
		인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)	암호화 저장
		내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부·적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보	암호화 저장(비밀번호는 일방향 암호화 저장) ※ 비밀번호는 일방향 암호화 저장	

-내부망에 주민등록번호를 저장하는 경우, 「개인정보 보호법」 제24조의2, 동법 시행령 제21조의2에 따라 「개인정보의 안전성 확보조치 기준」 제7조 제4항 (“개인정보 영향평가”나 “암호화 미적용시 위험도 분석”)와 관계없이 암호화 하여야 한다. 이 경우에는 다음의 기간 이전까지 암호화 적용을 완료하여야 한다.


※ 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일

※ 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

 [Q2]. 공공기관입니다. 개인정보처리시스템의 DBMS (DataBase Management System)에서 제공하는 TDE(Transparent Data Encryption) 방식을 사용한 암호화가 개인정보 보호법에 위배되니까?

개인정보 보호법 관점에서는 개인정보의 안전성 확보조치 기준(고시)에 따라 고유식별정보 암호화시 안전한 알고리즘을 사용하도록 하고 있습니다. TDE 방식에서 안전한 알고리즘을 사용하여 암호화한다면 법 위반 사항이 아닙니다.

다만, 공공기관은 전자정부법에 따라 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용하여야 하며 자세한 사항은 해당 기관에 적용되는 관련 법령, 고시, 규정, 지침 등을 확인하시기 바랍니다

 [Q3]. 암호화 관련하여 우리 기관(공공, 민간)에 적용되는 규정·지침과 개인정보보호법에서 적용하는 암호화 요구사항이 서로 다를 때 어느 것을 적용해야 하나요?

개인정보 보호법 및 시행령, 고시에서 규정한 암호화 요구사항을 준수하면 개인정보 보호법상 암호화 의무는 준수한 것입니다. 본 고시 준수로 인하여 다른 규정·지침을 준수하기 어렵게 된다면 “개인정보 보호법”은 준수 하였으나 해당 규정·지침은 위배한 것이 될 수 있습니다.

따라서, 최선의 방법은 개인정보 보호법과 해당 기관에 적용되는 규정·지침에서 요구하는 암호화 관련 사항 모두를 준수하는 것이라 할 수 있습니다.

 [Q4]. 안전한 암호 알고리즘에는 어떤 것들이 있나요?

안전한 암호 알고리즘은 국내·외 전문기관에서 권고하고 있는 알고리즘으로서 본 안내서의 [참고 1] 국내·외 암호 연구 관련 기관의 권고 암호 알고리즘, [참고 2] 국가정보원 검증대상 암호 알고리즘 목록의 내용을 참고하시기 바랍니다.

 [Q5]. 대칭키 암호 알고리즘 DES나 해쉬함수 MD5를 사용하면 안 됩니까?

DES와 MD5와 같은 암호 알고리즘의 경우 안전성 유지가 어려우므로 안전한 암호 알고리즘으로 볼 수 없어 권고하고 있지 않습니다.

안전한 암호 알고리즘은 본 안내서의 [참고 1] 국내·외 암호 연구 관련 기관의 권고 암호 알고리즘, [참고 2] 국가정보원 검증대상 암호 알고리즘 목록 내용을 참고하시기 바랍니다.

 [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 사용할 수도 있습니다.



[Q7]. 암호화해야 하는 바이오정보의 대상은 어디까지 인지요?

암호화하여야 하는 바이오정보는 식별 및 인증 등의 업무절차상 수집이 명확한 경우로 한정되며, 이와 무관하게 수집되는 이미지, 녹취 정보 등은 암호화 대상에서 제외됩니다. 예를 들어, 콜센터 등에서 업무절차상 주민등록번호 수집이 명확한 경우의 음성기록은 암호화 해야 하나, 단순 상담 시 저장되는 음성기록 등은 암호화 대상에서 제외될 수 있습니다.



[Q8]. 안전한 대칭키 암호화 알고리즘 사용시 암호키(비밀키)의 길이는 어떻게 설정해야 하나요?

암호키의 길이가 짧거나 사용되는 문자의 종류를 섞어 쓰지 않으면 암호화가 되었더라도 공격자가 쉽게 암호 해독을 할 수 있습니다. 암호해독이 어렵도록 암호키 설정시 문자, 숫자, 특수문자 등의 문자조합 방법과 문자열 길이, 사용기간 등의 암호키 작성 규칙을 정하여 운영하는 것이 바람직합니다.

특히 잘 알려진 영문자, 숫자(1234, 123456, love, happy, admin, admin1234) 등은 쉽게 유추 할 수 있으므로 사용하지 않도록 주의해야 합니다.



[Q9]. 회사에 고객들의 이름, 주소, 전화번호, 이메일, 비밀번호를 저장하고 있습니다. 암호화 대상이 무엇인가요?

개인정보의 안전성 확보조치 기준 고시에서 암호화 대상은 고유식별정보(주민등록번호, 여권번호, 운전면허 번호, 외국인등록번호), 비밀번호, 바이오정보입니다.

특히, 비밀번호의 경우에는 일방향(해쉬) 암호화하여 저장하시면 됩니다.



[Q10]. 부동산중개업을 하고 있습니다. 업무용 컴퓨터에 한글, 엑셀을 이용하여 주민등록번호를 처리 하고 있습니다. 암호화를 어떻게 해야 합니까?

PC에 저장된 개인정보의 경우 상용프로그램(한글, 엑셀 등)에서 제공하는 비밀번호 설정기능을 사용하여 암호화를 적용하거나, 안전한 암호화 알고리즘을 이용하는 소프트웨어를 사용하여 암호화할 수 있습니다.

※ 한글 오피스 : 파일 >> 다른이름으로 저장하기 >> 문서 암호 설정에서 암호 설정 가능
※ MS 오피스 : 파일 >> 다른이름으로 저장하기 >> 도구 >> 일반옵션에서 암호 설정 가능



[Q11]. A사가 개인정보처리시스템을 위탁하거나, ASP(Application Service Provider), 클라우드 서비스를 이용하는 경우 암호화 수행을 누가 해야 하나요?

개인정보의 암호화 등 안전성 확보조치는 원칙적으로 “개인정보처리자”의 의무입니다. 따라서 개인정보 처리시스템을 위탁하거나 ASP를 이용하는 경우에도 암호화 조치사항에 대한 이행여부에 대한 책임은 위탁기관인 A사가 지게 됩니다.

다만, A사는 암호화에 대한 요구사항을 A사의 위탁을 받은 수탁기관(ASP, 클라우드 서비스 제공자 등)과의 계약서 등에 명시하여 수탁기관으로 하여금 암호화를 처리하게 요구할 수 있습니다.

제2절 참고자료

[참고 1] 국내·외 암호 연구 관련 기관의 권고 암호 알고리즘

(2016년 9월 기준)

분류	미국(NIST)	일본(CRYPTREC)	유럽(ECRYPT)	국내
대칭키 암호 알고리즘	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 Blowfish KASUMI 3TDEA	SEED, HIGHT ARIA-128/192/256
공개키 암호 알고리즘 (메시지 암호·복호화)	RSA (사용 권고하는 키길이 확인 필요)	RSAES-OAEP RSAES-PKCS1	RSAES-OAEP RSAES-PKCS1	RSAES-OAEP
일방향 암호 알고리즘	SHA-224/256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-224/256/384/512

※ 국내·외 암호 연구 관련 기관에서 대표적으로 다루어지는 권고 암호 알고리즘만 표시

※ 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인 필요

※ 국내외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(<http://seed.kisa.or.kr>)의 “암호 표준화 및 유관 기관”에서도 확인 가능

[참고 2] 국가정보원 검증대상 암호 알고리즘 목록

(2016년 9월 기준)


분류		암호 알고리즘	참조표준
비밀키	블록암호	ARIA	<ul style="list-style-type: none"> • KS X 1213-1 128비트 블록 암호 알고리즘 ARIA-제1부 : 일반 (2009) • KS X 1213-1 128비트 블록 암호 알고리즘 ARIA-제2부 : 운영모드 (2014) • IETF RFC 5794, A Description of the ARIA Encryption Algorithm (2010)
		SEED	<ul style="list-style-type: none"> • TTAS.KO-12.0004/R1 128비트 블록 암호 알고리즘 SEED (2005) • TTAS.KO-12.0025 128비트 블록 암호 알고리즘 SEED의 운영모드 (2003) • ISO/IEC 18033-3 Information technology - Security techniques - Encryption - Part 3: Block ciphers (2010)
		LEA	<ul style="list-style-type: none"> • TTAK.KO-12.0223 128비트 블록 암호 알고리즘 LEA (2013) • TTAK.KO-12.0246 128비트 블록 암호 LEA 운영모드 (2014)
		HIGHT	<ul style="list-style-type: none"> • TTAS.KO.12.0040/R1 64비트 블록 암호 알고리즘 HIGHT (2008) • TTAK.KO-12.0166 64비트 블록 암호 알고리즘 HIGHT 운영모드 (2011) • ISO/IEC 18033-3 Information technology - Security techniques - Encryption - Part 3: Block ciphers (2010)
	블록암호 운영모드	기밀성 (ECB, CBC, CFB, OFB, CTR)	<ul style="list-style-type: none"> • KS X 1213-2 128비트 블록 암호 알고리즘 ARIA-제2부 : 운영모드 (2014) • TTAS.KO-12.0025 블록암호알고리즘 SEED의 운영모드 (2003) • TTAK.KO-12.0246 128비트 블록 암호 LEA 운영모드 (2014) • TTAK.KO-12.0166 64비트 블록 암호 알고리즘 HIGHT 운영모드 (2011)
		기밀성/인증 (CCM,GCM)	<ul style="list-style-type: none"> • TTAS.KO-12,0131 기밀성과 메시지 인증을 제공하는 128비트 블록 암호알고리즘 운영모드 (2010)
해시함수		SHA-224, SHA-256, SHA-384, SHA-512	<ul style="list-style-type: none"> • ISO/IEC 10118-3 Information technology - Security techniques - Hash-functions - Part 3 : Dedicated hash-function 8 (SHA-224) (2006)
메시지 인증	해시기반	HMAC	<ul style="list-style-type: none"> • ISO/IEC 9797-2 Information technology - Security techniques - Message Authentication Codes(MACs) - Part 2 : Mechanism using a dedicated hash-function (2011)
	블록기반	CMAC, GMAC	<ul style="list-style-type: none"> • KS X 1213-2 128비트 블록 암호 알고리즘 ARIA-제2부 : 운영모드 (2014) • TTAK.KO-12.0246 128비트 블록 암호 LEA 운영모드 (2014) • TTAS.KO-12.0131 기밀성과 메시지 인증을 제공하는 128비트 블록암호알고리즘 운영모드 (2010) • ISO/IEC 9797-1 Information technology - Security techniques - Message Authentication Codes(MACs) - Part 1 : Mechanism using a block cipher (2011)

난수발생기		CTR_DRBG, HASH_DRBG, HMAC_DRBG	<ul style="list-style-type: none"> TTAK.KO-12.0189 결정론적 난수발생기 - 제1부 - 블록 암호 기반 난수발생기 (2015) TTAK.KO-12.0190 결정론적 난수발생기 - 제2부 - 해시 함수 기반 난수발생기 (2012) TTAK.KO-12.0191 결정론적 난수발생기 - 제3부 - HMAC 기반 난수발생기 (2012) ISO/IEC 18031 Information technology - Security techniques - Random bit generation (2011)
공개키 암호	공개키 암호	RSAES	<ul style="list-style-type: none"> ISO/IEC 18033-2 Information technology - Security techniques - Encryption algorithms - Part 2 : Asymmetric cipher (2006)
	파라미터	RSAES	<ul style="list-style-type: none"> 공개키 길이 : 2048, 3072
전자 서명	전자서명	RSA-PSS	<ul style="list-style-type: none"> ISO/IEC 14888-2 Information technology - Security techniques - Digital signatures with appendix - Part 2 : Integer factorization based mechanisms (2008)
		ECDSA, KCDSA, EC-KCDSA	<ul style="list-style-type: none"> ISO/IEC 14888-3 Information technology - Security techniques - Digital signatures with appendix - Part 3 : Discrete algorithm based mechanisms (2006) TTAS.KO-12.0001/R1 부가형 전자서명 방식 표준 - 제2부 : 인증서 기반 전자서명 알고리즘 (2000) TTAS.KO-12.0015 부가형 전자서명 방식 표준 - 제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘 (2001)
	파라미터	RSA-PSS	<ul style="list-style-type: none"> 공개키 길이 : 2048, 3072
		KCDSA	<ul style="list-style-type: none"> (공개키 길이, 개인키 길이) : (2048,224), (2048, 256) ISO/IEC 11770-3 Information technology - Security techniques - Key management - Part 3 : Mechanisms using asymmetric techniques (2008)
		ECDSA, EC-KCDSA	<ul style="list-style-type: none"> B-233, B-283, K-233, K-283, P-224, P-256 NIST FIPS 186-3 Digital Signature Standard(DSS)

※ 검증대상 암호 알고리즘 목록은 국가정보원 홈페이지(16.9월 기준)에 나와있는 검증대상 암호알고리즘(<http://www.nis.go.kr/AF/1.7.3.2.do>)이므로 최신 정보 확인 필요

[참고 3] 다른 법률에서의 암호화 관련 규정

1. 전자정부법

 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 소속기관, 지방자치단체 및 공공기관을 대상으로 하며, 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법, 행정기관의 정보통신망, 행정정보 등의 안전성 확보를 위한 보안대책 등을 규정하고 있다.

전자정부법

• 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.

전자정부법 시행령

• 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·운영
 - 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.

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

 정보통신서비스 제공자(기간통신사업자, 별정통신사업자, 부가통신사업자), 방송사업자 등이 적용 대상으로 하며, 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함을 목적으로 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

• 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(개인정보의 보호조치)

- ④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.
 1. 비밀번호의 일방향 암호화 저장
 2. 주민등록번호, 계좌정보 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 정하여 고시하는 정보의 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.





개인정보의 기술적·관리적 보호조치 기준(방송통신위원회 고시, 제2015-03호)

• 제6조(개인정보의 암호화)

- ① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.
- ② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.
 - 1. 주민등록번호
 - 2. 여권번호
 - 3. 운전면허번호
 - 4. 외국인등록번호
 - 5. 신용카드번호
 - 6. 계좌번호
 - 7. 바이오정보
- 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 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

3. 신용정보의 이용 및 보호에 관한 법률



신용조회업, 채권추심업 등 신용정보업(회사), 신용정보집중기관 및 신용정보제공·이용자 등을 적용 대상으로 하며, 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모하며 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 한다.



신용정보의 이용 및 보호에 관한 법률

• 제19조(신용정보전산시스템의 안전보호)

- ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공통전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.
- ② 신용정보제공·이용자가 다른 신용정보제공·이용자 또는 신용조회회사와 서로 이 법에 따라 신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 신용정보 보안관리 대책을 포함한 계약을 체결하여야 한다.



신용정보의 이용 및 보호에 관한 법률 시행령

· 제16조(기술적·물리적·관리적 보안대책의 수립)

- ① 법 제19조제1항에 따라 신용정보회사등은 신용정보전산시스템의 안전보호를 위하여 다음 각 호의 사항이 포함된 기술적·물리적·관리적 보안대책을 세워야 한다.
1. 신용정보에 제3자가 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영에 관한 사항
 2. 신용정보전산시스템에 입력된 정보의 변경·훼손 및 파괴를 방지하기 위한 사항
 3. 신용정보 취급·조회 권한을 직급별·업무별로 차등 부여하는 데에 관한 사항 및 신용정보 조회기록의 주기적인 점검에 관한 사항
 4. 그 밖에 신용정보의 안정성 확보를 위하여 필요한 사항
- ② 금융위원회는 제1항 각 호에 따른 사항의 구체적인 내용을 정하여 고시할 수 있다.



신용정보업감독규정

· 제20조(기술적·물리적·관리적 보안대책)

영 제16조제2항에 따라 신용정보회사등이 마련해야 할 기술적·물리적·관리적 보안대책의 구체적인 기준은 별표 3과 같다.

[별표 3] 기술적·물리적·관리적 보안대책 마련 기준

II. 기술적·물리적 보안대책

3. 개인신용정보의 암호화

- ① 신용정보회사등은 비밀번호, 바이오정보 등 본인임을 인증하는 정보는 암호화하여 저장하며, 이는 조회할 수 없도록 하여야 한다. 다만, 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.
- ② 신용정보회사등은 정보통신망을 통해 개인신용정보 및 인증정보를 송·수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.
 1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인신용정보를 암호화하여 송·수신하는 기능
 2. 웹서버에 암호화 응용프로그램을 설치하여 개인신용정보를 암호화하여 송·수신하는 기능
- ③ 신용정보회사등은 개인신용정보를 PC에 저장할 때에는 이를 암호화해야 한다.
- ④ 신용정보회사등은 다음 각 호의 기준에 따라 주민등록번호의 암호화 등의 조치를 취하여야 한다.
 1. 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달하는 경우에는 암호화하여야 한다.
 2. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 저장할 때에는 암호화하여야 한다.
 3. 신용정보회사등이 내부망에 주민등록번호를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
 - 가. 「개인정보 보호법」 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과나 그 밖의 신용정보회사등의 경우에는 개인신용정보처리시스템에 적용되고 있는 개인신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석한 결과
 4. 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.
- ⑤ 신용정보집중기관과 신용조회회사가 서로 개인식별번호를 제공하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.
- ⑥ 신용정보회사등이 개인신용정보의 처리를 위탁하는 경우 개인식별번호를 암호화하여 수탁자에게 제공하여야 한다.