금보원 2014-14

DB 암호화 기술 가이드

2014. 12

금융보안연구원
Financial Security Agency

제·개정 이력

순번	제·개정일	제·개정 내역
1	2012.9	- 최초 작성 ('DB 암호화 최신동향 및 보안기술 분석 보고서 ')
2	2014.12	- 사고사례 및 통계 내용 삭제 - 법률 및 규정 내용 추가 - 기술 동향 수정 - 도입 시 고려사항 수정 및 추가 - 구축 방안 수정

차례

DB 암호화 기술 가이드

차례

DB 암호화 기술 가이드

그림

DB 암호화 기술 가이드

표

DB 암호화 기술 가이드

표

DB 암호화 기술 가이드

제1장 개 요

데이터베이스(이하 'DB')는 여러 시스템을 통해 접근이 가능한 공유된 형태의 통합된 데이터 집합으로 데이터를 수집하고 가공하여 서비스하는 것을 목적으로 한다. 오늘날 기업들은 다양한 서비스 제공을 위해 고객의 많은 정보를 보유하고 있는 가운데 최근에는 카드사 고객정보 유출 사건 등 잇따른 개인정보 유출 사건들이 발생하고 있어, 이용자들의 보안에 대한 요구가 커지고 'DB 보안'의 필요성 또한 날로 높아지고 있다.

이로 인해 정책 또한 변화하여 주민등록번호를 암호화하는 것이 의무화되었고, 개인정보 유출 시 기업의 처벌 및 과징금 부과 규정이 강화되는 등 다시금 'DB 보안'에 대한 중요성이 강조되고 있다.

'DB 보안' 기술은 기업의 성격, 규모, 특징 및 데이터의 중요도에 따라 관리적, 기술적 방법 등 다양한 형태로 적용될 수 있으며, 이를 위한 주요 기술로는 DB 데이터를 암호화 하는 것이 있다. 이 기술은 비인가자에 의한 데이터 오용을 방지하고 정보가 유출되더라도 이용 및 유통 등 2차 피해 가능성을 낮출 수 있으며, 본 가이드에서는 이러한 'DB 암호화' 기술 도입 시 고려사항들을 중점으로 기술한다.

본 가이드의 구성은 다음과 같다.

2장은 DB 암호화 관련 법·규정 및 위협 동향에 대해 기술하였고, 3장은 국내에 알려진 DB 암호화 기술들에 대하여 소개하였다. 4장에서는 다양한 DB 암호화 기술 도입 시 공통적으로 고려해야 할 사항, 5장에서는 실제 DB 암호화 기술 적용 시 구축 방안에 대해 기술하였다.

기업에서는 'DB 암호화' 기술을 적용 시 현재 제공하고 있는 서비스의 안전성을 도모하고 고객 및 기업의 정보를 보호하는 기술의 하나로써 그 보안 범위를 명확히 하고 세분화하여 구축하여야 할 것이다. 또한, 전반적인 DB 보안 체계를 갖추기 위해서 'DB 암호화' 기술 뿐 아니라 외부 및 내부 위협에 대응하기 위한 다양한 보안 기술들을 고려하여 심층적인 보안체계를 구축하여야 할 것이다.

제2장

관련 법·규정 및 위협 동향

1. 관련 법·규정

DB 암호화와 관련된 법률 및 규정은 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법), 전자금융감독규정, 신용정보업감독규정 등이 있다. 이들 법률 및 규정의 DB 암호화 관련 내용들을 간단히 살펴보면 다음 [표 1]과 같다.

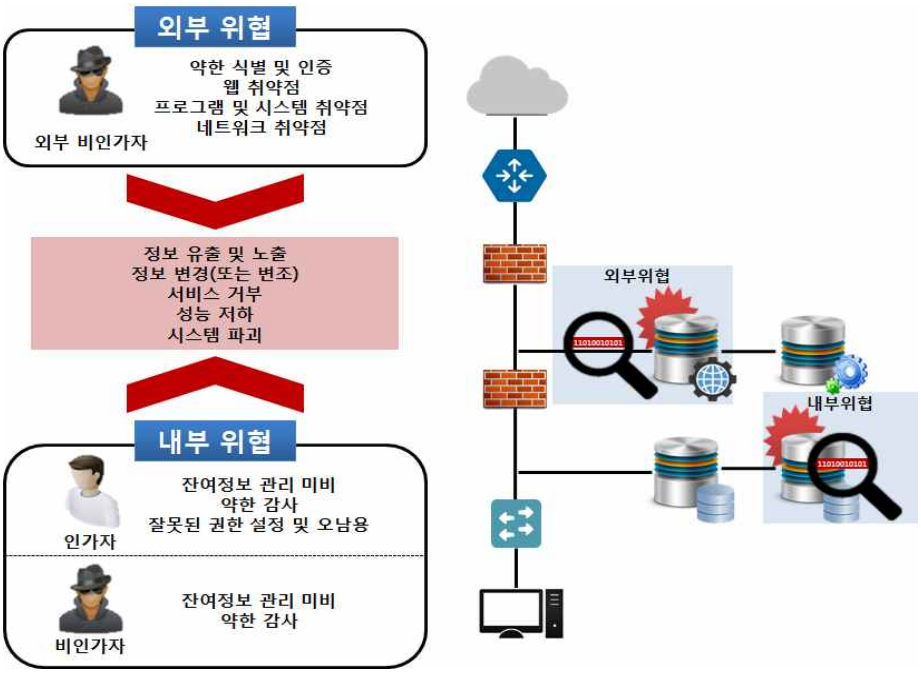
[표 1] DB 암호화 관련 법률[1)]

구분	내용
개인정보보호법 (제24조 3항, 24조의2 2항, 29조)	고유식별정보를 처리하는 경우에 그 주민등록번호를 포함한 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 등 안전성 확보에 필요한 조치를 하도록 함
정보통신망법 (제28조 1항)	개인정보의 보호조치로 기술적·관리적 조치를 하여야 하며, 그 기준으로 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안조치를 하도록 함
전자금융감독규정 (제17조 1항, 제32조, 제33조 1항)	DMZ구간 내에 거래로그를 관리하기 위한 경우 암호화하여 저장·관리하고, 내부사용자 및 이용자 비밀번호를 암호화하여 보관하도록 함
신용정보업감독규정 (제 20조, [별표 3])	신용정보회사등은 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해서는 복호화되지 않도록 일방향 암호화하여 저장하여야 함

1) 상세 내용에 대해서는 '[붙임 2] 관련 법률 및 규정' 참고

2. DB 보안 위협

기업의 많은 정보를 보유하고 있는 DB는 천재지변, 시스템 장애, 사용자의 실수, 악의적인 의도 등 다양한 원인으로 인해 외·내부에서 위협이 발생할 수 있다.



(그림 1) DB 보안 위협

가. 외부 위협

DB의 외부 위협은 천재지변에 의한 DB의 물리적 손상 외에 악의적인 의도를 가지고 DB의 취약점을 공격하는 위협이 주를 이루며, 내부의 인가된 사용자로 위장이 가능한 약한 식별 인증 및 감사 정책, 웹 취약점, DBMS(DataBase Management System)의 프로그램 및 시스템의 취약점,

네트워크상의 취약점(통신 암호화 미비 등)을 활용하여 정보 유출 및 노출, 정보 변경, 서비스 거부, 성능 저하 등의 문제를 유발할 수 있다.

[표 2] 외부 위협 분류

보안위협	설명
약한 식별 및 인증	정당한 사용자 신원을 획득하기 위해 반복적인 인증 시도 및 사회공학적 기법 등을 이용하여 인가된 사용자 신원을 획득하고 정보 유출 및 변경, 서비스 거부 등 DB시스템 공격 가능
웹 취약점	SQL Injection 공격, File Upload 취약점, 파라미터 변조 취약점 등을 통한 불법적인 정보 획득
프로그램 및 시스템 취약점	DBMS 설계 결함, 어플리케이션의 취약점 등으로 인해 정보 유출, 장애 발생
네트워크 취약점	스니핑 공격 또는 DoS 공격 등을 통해 정보 유출, 데이터 및 시스템 파괴, 변경 또는 서비스 지연 등 유발

(1) 약한 식별 및 인증

사용자 식별 및 인증은 DB의 데이터를 접근하기 위한 가장 기본적인 단계이다. 약한 인증 수준과 식별되기 쉬운 비밀번호를 사용한다면 사전 공격(Dictionary Attack), 무작위 대입 공격(Brute Force Attack), 사회 공학적 기법(Social Engineering)을 통하여 식별 및 인증 정보가 쉽게 노출될 수 있다. 이런 공격방법을 활용하여 인가된 사용자의 신원을 획득하고, 정보 유출 및 변경, 서비스 거부 등의 문제를 유발할 수 있다.

(2) 웹 취약점

외부의 인가되지 않은 사용자가 악의적인 목적을 가지고 웹서버의 취약점을 활용하여 DB의 중요정보 유출을 시도할 수 있다.

개발자가 의도하지 않은 SQL문을 실행하여 DB를 조작하는 SQL Injection 공격 수행, 파라미터 변조 취약점 활용, File Upload에 대한 취약점을 활용한 웹쉘(Web Shell) 실행 등 웹 취약점을 통해 DB 데이터를 열람 및 유출하거나 DB 서버에 시스템 명령을 실행하는 것이 가능할 수 있다.

(3) 프로그램 및 시스템 취약점

DBMS 설계 결함 및 프로그램 버그, DB의 OS 및 시스템에 설치된 추가 서비스들에 내재된 보안 취약점(소프트웨어 업데이트 및 패치 미수행 등) 을 통해 비인가된 접근, 데이터 유출 및 변조, 장애 등이 발생할 수 있다.

(4) 네트워크 취약점

외부에 인가되지 않은 사용자는 DB와 통신하는 네트워크 취약점을 활용하여 네트워크상의 정보를 절취(유출)하는 스니핑 공격, DoS공격 등이 가능할 수 있다. DoS공격은 시스템이 처리할 수 있는 능력 이상의 정보를 요청 또는 네트워크 용량을 초과시켜 시스템의 정상적인 기능 수행을 방해하고 인가된 사용자에 의한 합법적인 접근을 불가능하게 하는 공격으로 데이터 및 시스템 파괴, 변경 또는 서비스 지연 등의 문제를 일으킨다.

나. 내부 위협

DB의 내부 위협은 내부의 인가자와 비인가자에 의한 위협으로 구분할 수 있다. 잔여정보 관리 미비, 약한 감사 수행, 잘못된 권한 설정 등 내부 관리자 및 사용자의 실수 또는 부주의로 인해 DB의 정보가 유출(노출)될 수 있으며, 인가된 내부 관리자 및 사용자라고 하더라도 자신의 권한을 오남용하여 이와 같은 문제를 유발할 수 있다.

[표 3] 내부 위협 분류

보안위협	설명
잔여정보 관리 미비	DB 로그 등 잔여 정보를 관리하지 않아 불법적인 데이터 획득 및 유출 가능
약한 감사	약한 감사 정책은 악의적인 DB 접근 시도 시 사용자 추적을 어렵게 함
잘못된 권한 설정 및 오남용	사용자에게 권한을 더 많이 부여하여 인가되지 않은 작업 수행이 가능, 인가된 사용자도 권한을 오남용하여 정보 유출 및 변조 가능

(1) 잔여 정보 관리 미비

DB 로그 및 잔여 정보 관리를 하지 않는 경우 잔여 정보를 이용하여 데이터를 획득할 수 있으며, 로그에 민감한 정보를 포함하는 경우 로그를 통하여 중요 정보가 유출 될 수 있다. 또한 어플리케이션의 동작 상태를 확인하기 위한 로그정보 생성 시에도 민감한 데이터가 노출되지 않도록 주의하여야 한다.

(2) 약한 감사

DB의 감사 수준을 낮게 설정하여 제한된 감사정보를 기록하는 경우 악의적인 사용자의 데이터 접근 및 사용, 탐지 및 추적, 복구에 어려움이 있다. 높은 감사는 일반적으로 시스템 자원을 많이 사용하여 성능 저하를 가져오기 때문에 가용성을 고려하여 설정하여야 하지만, 민감도가 높은 데이터에 접근하는 트랜잭션의 경우에는 사용자의 신원, 시간, IP, 데이터 접근 및 조작에 대한 감사 기록을 남기는 것이 필요하다.

특히, 악의적인 목적을 가진 관리자가 감사 수준을 변경하여 감사 기록을 남지 않도록 하거나, 감사 기록을 변조하는 위협이 발생할 수 있기 때문에 DB 관리자와 감사자의 직무를 분리하여 관리자에 의한 악의적인 접근 및 내부 정보 유출에 대비하여야 한다.

(3) 잘못된 권한 설정 및 오남용

DB의 데이터 접근 권한이 업무 사용을 위해 허용된 권한보다 더 많이 부여되거나 정당한 사용자가 악의적인 목적으로 허용된 범위를 넘어서 인가되지 않은 작업을 수행하는 경우에 권한을 오·남용하여 데이터 유출 또는 데이터 변조할 수 있다.

제3장 기술 동향

DB의 데이터를 암호화할 수 있는 방식은 일반적으로 컬럼 암호화 방식과 블록 암호화 방식으로 나눌 수 있다. 컬럼 암호화 방식은 암·복호화 위치에 따라 Plug-In, API 및 혼합 방식인 Hybrid 등의 방식이 있고 블록 암호화 방식은 TDE, 파일 암호화 방식이 있다. 아래 [표 4]는 이러한 DB 암호화 유형들에 대한 특징을 설명한다.

[표 4] DB 암호화 기술 방식별 특징

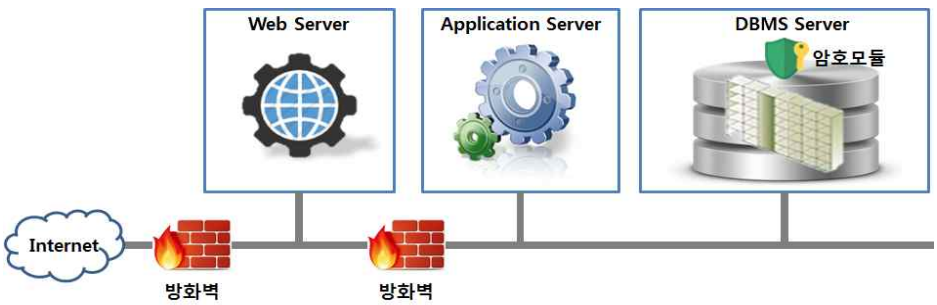
구분	방식	운영 형태	특징
컬럼 암호화	Plug-In	DB 서버	구축 시 일부 어플리케이션 수정이 필요하며 DB 서버의 성능에 대한 검토 필요
	API	DB & 어플리케이션 서버	Plug-In 방식에 비해 DB 서버에 영향을 주지 않으나 구축 시 어플리케이션의 수정 필요
	Hybrid (Plug-In +API)	DB & 어플리케이션 서버	Plug-In과 API 방식이 조합된 형식임
블록 암호화	TDE 방식	DB 서버	일반적으로 어플리케이션 수정이 필요 없음, DB의 지원 가능 여부 확인 필요
	파일 암호화	DB & 어플리케이션 서버	일반적으로 어플리케이션 수정이 필요 없음, OS의 지원 가능 여부 확인 필요
기타		DB or 어플리케이션 서버	컬럼 사이즈 증가, 성능 이슈 등 보완 필요

※ 기타 : Token 방식, Secure Proxy 방식, Filter 방식, Appliance 방식 등

1. Plug-In 방식

Plug-In 방식은 암·복호화 모듈을 DB 서버 내에 설치하고 이곳에서 암·복호화를 수행하는 구조로, 적용성이 뛰어나지만 암·복호화 시 DB 서버의 CPU를 사용하기 때문에 부하가 발생할 수 있다. 그러므로 트랜잭션 처리량이 많지 않아 성능에 대한 민감성이 낮은 시스템의 경우 저렴한 비용으로 구축할 수 있다. 어플리케이션 서버에서 DB계정이 탈취될 경우 복호화된 평문 데이터 유출이 가능하므로 이에 대한 보안 조치가 필요하며, 암호화 컬럼 사이즈 증가, 성능 이슈 등이 있는 경우 일부 어플리케이션을 수정하여 적용이 가능하다.

Plug-In 방식의 구성에서 DB의 테이블 또는 컬럼 단위의 암호화를 적용하면 암호화된 테이블 이용을 위하여 추가적인 Object들이 생성되므로, 운영 및 백업 등 DB에 관련된 작업을 수행할 때 이러한 Object들을 함께 고려하여야 한다.



(그림 2) Plug-In 방식의 구성 예

[표 5]는 Plug-In 방식의 DB 암호화 제품이 제공하는 기능을 보여준다.

[표 5] Plug-In 방식의 기능

항 목	내용
암호 알고리즘	SHA-256/384/512 및 키 길이 128bit 이상의 AES, TDES, SEED, ARIA 등 지원
암·복호화 위치	DB 서버
DB서버의 부하	높음*
색인 검색	가능, 별도 인덱스 기능 필요
배치 처리	가능
어플리케이션	수정 없이 적용할 수 있는 구조이나 암호화 컬럼 사이즈 증가, 성능 이슈 등이 있는 경우 일부 수정 필요
접근통제	DB에 접속하는 DB클라이언트에서 사용자 식별 가능

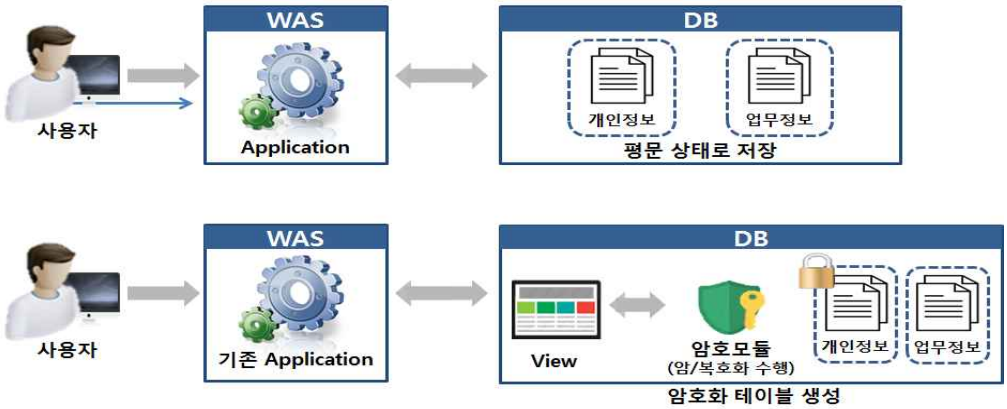
* DB 암호화 기술 적용에 따른 서버의 추가 부하는 '높음 / 보통 / 낮음'으로 구분하여 기술하였음

가. View

Plug-In 방식의 구성에서 테이블/컬럼을 암호화하게 되면 기존 테이블 이름과 동일한 View와 변경된 이름의 암호화된 테이블이 생성되고, 암호화 전 원본 테이블은 삭제하게 된다.

암호화 후 생성된 View는 암호화 된 데이터를 복호화하여 보여주는 통로 역할을 한다. View 이름을 암호화하기 전의 테이블 이름과 같게 생성함으로써 원본 테이블을 사용하던 기존 어플리케이션의 쿼리를 수정 없이 또는 수정을 최소화하여 사용이 가능하도록 하며, 권한이 있는 사용자가 복호화된 데이터를 간편하게 사용할 수 있도록 만들어 준다. 또한 DML[2]을 사용하는 사용자의 유형을 체크하여 쿼리를 제한하는 등의 기능을 수행 할 수 있다.

2) DML : Data Manipulation Language



(그림 3) Plug-In 방식 암호화 개념도

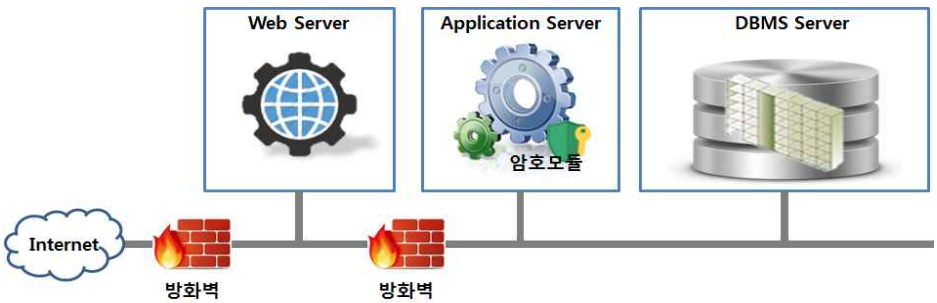
나. Trigger

Trigger의 역할은 복호화 View에 DML요청이 들어오는 경우 평문 데이터를 암호화시켜 암호화 테이블에 DML처리를 하는 역할을 한다. View에 암호화 Trigger를 연결시켜줌으로써 기존 어플리케이션 및 사용자의 DML 쿼리를 수정 없이 또는 최소화하여 사용할 수 있도록 한다.

2. API 방식

API방식은 암·복호화 모듈을 어플리케이션 서버 내에 설치하고 이곳에서 암·복호화를 수행하는 구조로 어플리케이션의 수정을 동반한다. 따라서 API 방식의 DB 암호화 기술 도입은 기존에 운영 중인 시스템에 적용하기보다 차세대 시스템 개발 등 기존 어플리케이션에 대한 전면적인 수정이 가능한 경우 적용하면 효과적이다. (그림 4)와 같이 API 방식의 구성에서는 DB시스템의 영향도가 낮고 DBMS의 부하를 분산하는 효과가 있으며, 어플리케이션 서버에서 DB계정이 탈취되더라도 데이터가 암호화되어 있기 때문에 유출 위험이 적지만 각각의 어플리

케이션 서버에서 암복호화 처리를 수행하므로 중앙화된 접근 통제가 어렵다. Plug-In방식에 비해 암복호화 속도가 빨라 대용량 온라인 트랜잭션 서비스 등에 적용 가능하나, 어플리케이션 수정으로 인해 소요되는 인력 및 시간은 API방식이 가장 많이 소요된다.



(그림 4) API 방식의 구성 예

다음 [표 6]은 API 방식에서 제공하는 기능들을 나타낸다.

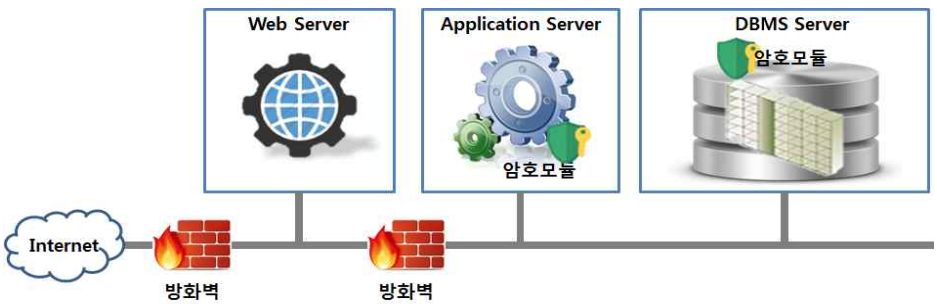
[표 6] API 방식의 기능

항 목	내용
암호 알고리즘	SHA-256/384/512 및 키 길이 128bit 이상의 AES, TDES, SEED, ARIA 등 지원
암·복호화 위치	어플리케이션 서버 (DB 서버가 어플리케이션 기능을 수행 할 경우 DB 서버에서 암복호화 가능)
DB 서버 부하	낮음(어플리케이션 서버에 부하 발생)
색인 검색	일치검색 가능, 부분일치검색 불가(부분 암호화 시 가능)
배치 처리	가능
어플리케이션	어플리케이션의 소스(암호화 테이블과 관련된 부분)를 수정해야 함
접근통제	암복호화 작업이 어플리케이션 서버 상에서 수행되기 때문에 DB 접속정보를 통한 사용자 식별은 불가, 어플리케이션 서버에 접속하는 서비스 접속자만 식별 가능

3. Hybrid 방식

Plug-In 방식의 단점인 배치 업무의 성능 저하를 보완하기 위해 API 방식을 이용하는 구성으로서, 일반적으로는 아래의 (그림 5)와 같이 일부 SQL은 API 방식을 이용하여 최적의 성능을 보장하도록 하고, 나머지 대부분은 DB내의 Plug-In 방식을 이용하여 어플리케이션 수정을 최소화 하도록 암·복호화 모듈을 DB 서버와 어플리케이션 서버에 설치한다.

어떤 어플리케이션에 API 방식을 적용할 것인지에 대한 분석은 기존 시스템에서 수행되는 SQL정보를 수집 및 분석하는 방법을 활용할 수 있다. 특정 기간 동안 암호화 대상 DBMS에서 수행된 모든 SQL 정보를 수집한 후, 각 SQL별로 사용한 테이블/컬럼, DB 암호화 적용 시 영향을 받는 SQL 사용 빈도, CPU, Memory, Storage 등의 영향도를 파악하여 SQL을 사용하는 프로그램에 대해 API방식을 적용하면 적용대상을 최소화하면서 효과를 높일 수 있다.



(그림 5) Hybrid 방식의 구성 예

다음의 [표 7]은 Hybrid 방식에서 지원하는 기능들을 나타낸다.

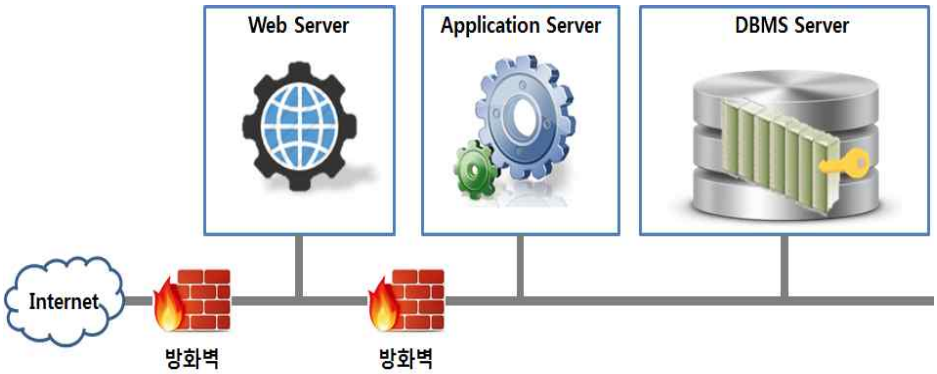
[표 7] Hybrid 방식의 기능

항 목	내용
암호 알고리즘	SHA-256/384/512 및 키 길이 128bit 이상의 AES, TDES, SEED, ARIA 등 지원
암·복호화 위치	어플리케이션 서버 및 DB 서버
DB 서버 부하	보통
색인 검색	가능
배치 처리	가능(Plug-In방식에 비해 API방식이 대량 데이터 처리에 용이하여 API방식 활용)
어플리케이션	API를 적용하는 부분은 소스 수정 필요

4. TDE 방식

DBMS에 추가 기능으로 제공되는 암호화 기능을 이용하여 DB 내부에서 데이터 파일 저장 시 암호화하고, 파일에 저장된 내용을 메모리 영역으로 가져올 때 DBMS에 의해 자동으로 복호화되는 방식으로서, DBMS(Oracle[3], MS SQL 등) 종류 및 버전에 따라 기능 지원 여부가 다르다. DBMS Kernel 레벨에서 처리되므로 어플리케이션에 대한 수정이 없고 인덱스의 경우 DBMS 자체 인덱스 기능과 연동이 가능하다. 암호화로 인해 기존 시스템에 미치는 영향이 적고 성능이 뛰어나지만, DBMS에 로그인한 사용자 중 암호화된 데이터에 접근 권한이 있는 모든 사용자에게 암호화된 정보가 복호화되어 조회되므로, 이에 대한 보완책으로 실시간 마스킹 기능 등을 함께 고려하여야 한다.

3) Oracle 11g에서는 테이블스페이스 단위 암호화 지원



(그림 6) TDE 방식의 구성 예

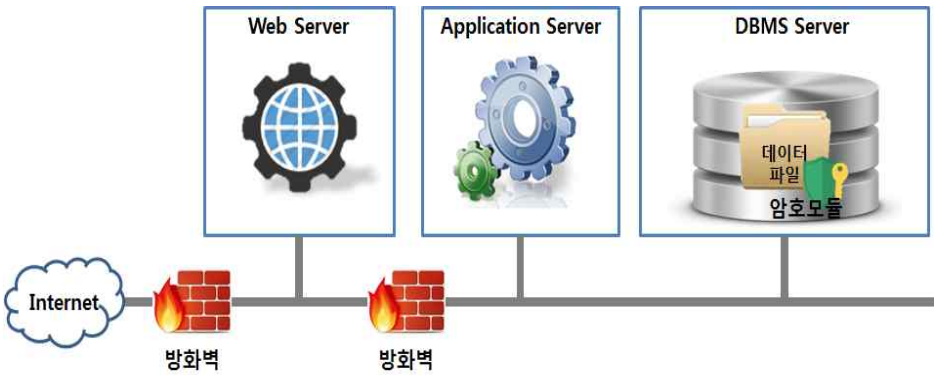
다음의 [표 8]는 TDE 방식에서 지원하는 기능들을 보여준다.

[표 8] TDE 방식의 기능

항 목	내용
암호 알고리즘	SHA-256/384/512 및 키 길이 128bit 이상의 AES, TDES 등 지원
암·복호화 위치	DB 서버
DB 서버 부하	낮음
색인 검색	가능(DBMS 연동)
배치 처리	가능
어플리케이션	수정 없음
접근통제	DB자체 ACL에 의해 DB계정만 통제하여 접근권한이 있는 DB사용자들은 복호화된 데이터 열람 가능

5. 파일 암호화 방식

파일 암호화 방식은 OS상에서 확인이 가능한 개체인 파일을 암호화하는 방식이다. OS에 대한 의존도가 높으나, 파일에 대해 직접적으로 암호화를 수행하므로 DB의 데이터 파일 뿐 아니라 로그파일, 이미지파일, 음성/영상 등의 비정형 데이터에 대한 암호화 적용이 가능하다. 이 방식으로 구성하면 어플리케이션의 수정이 없고, 인덱스의 경우 DBMS 자체 인덱스 기능을 사용할 수 있으며, 거의 모든 DBMS에 적용이 가능하나 TDE 방식과 마찬가지로 DBMS에 로그인한 모든 사용자에게 암호화된 정보가 복호화되어 조회되므로 마스킹 기능 도입 등 이를 보완하는 방안도 함께 고려하여야 하며, OS에 따라 지원 여부가 달라지기 때문에 사전에 확인이 필요하다.



(그림 7) 파일 암호화 방식의 구성 예

다음의 [표 9]는 파일 암호화 방식에서 지원하는 기능들을 나타낸다.

[표 9] 파일 암호화 방식의 기능

항 목	내용
암호 알고리즘	SHA-256 및 키 길이 128bit 이상의 AES, TDES, ARIA 등 지원
암·복호화 위치	DB 서버(OS커널)
DB 서버 부하	낮음
색인 검색	가능
배치 처리	가능
어플리케이션	수정 없음
접근통제	OS계정 및 응용 프로그램 단위로 접근 통제 수행, DB 내에 존재하는 DB사용자들은 복호화된 데이터 열람 가능

6. 기타 방식

가. Token 방식

데이터의 숫자나 형태, 구조를 그대로 유지하면서 난수와 같은 임의의 Token(대체값)과 별도의 테이블에 저장한 암호화 데이터를 연결하고 평문데이터의 일부 또는 전체를 Token으로 대체하여 원본 데이터의 식별이 불가능하도록 하는 방식으로 Hybrid 방식과 같이 DB 서버 또는 어플리케이션 서버에서 암·복호화 작업이 가능하다. Token의 데이터 타입을 원래 암호화 대상 데이터 타입과 동일하게 설정하면 기존 테이블의 구조를 변경하지 않아도 되며, 암호화 이후 컬럼 사이즈가 변경되지 않아 DB 서버 및 Memory 증설 등이 필요하지 않다. 다만 Token 값과 암호화 데이터를 저장하기 위한 별도의 관리 서버가 필요할 수 있으며, 일부 API 방식의 어플리케이션에 한하여 수정 및 변경이 필요하다.

이러한 Token 방식을 적용할 때에는 데이터 값을 대체하는 난수의 생성 방식이 원본 데이터를 유출할 수 없는 알고리즘으로 구성되었는지 보안성 측면의 검토가 필요하다.

나. Secure Proxy 방식

독립된 프로세스로 구동하여 어플리케이션과 DBMS 중간에서 암·복호화 처리를 하는 방식으로 Plug-In 방식과 동일하게 DBMS에서 암·복호화를 수행하나 View 또는 Trigger를 사용하지 않고 암·복호화 함수를 사용하여 원 테이블의 데이터를 입력 또는 조회할 수 있다. DB 서버 부하 등을 보완하기 위해 암·복호화 작업을 수행하는 Agent를 별도의 서버에 탑재하여 암·복호화 작업을 수행하는 것이 가능하나 보안 및 관리에 대해 추가적인 고려가 필요하다.

다. Filter 방식

독립된 프로세스로 구동하여 어플리케이션과 DBMS 중간에서 암·복호화 처리를 하는 방식으로 API 방식과 동일하게 어플리케이션 서버에서 암·복호화 처리를 하는 방식이다. JAVA기반의 어플리케이션에서 소스 수정 없이 암·복호화 할 수 있다. 하지만 등록된 SQL만 암·복호화가 가능하여 암·복호화 대상이 되는 SQL의 수집 및 변경이 필요하다. 암·복호화 작업을 수행하는 Agent를 별도의 서버에 탑재하여 암·복호화 작업을 수행하는 것이 가능하나 보안 및 관리에 대해 추가적인 고려가 필요하다.

라. Appliance 방식

어플리케이션 서버와 DB서버 사이에 Appliance 장비를 설치(Inline 또는 Proxy 방식으로 구성 가능)하여 해당 장비에서 테이블 컬럼 분석을 통해 암·복호화 컬럼 여부를 파악하여 실시간으로 암·복호화

처리 및 키 관리가 수행되는 방식이다. 어플리케이션 수정 및 변경을 수행하지 않고 구현이 가능하고, 필요 시 DB 서버 또는 어플리케이션 서버에 별도의 Agent 설치하여야 한다. Appliance 장비에서 암·복호화 및 키 관리가 수행되어 암·복호화 및 키 관리에 대한 보안성이 높고 암호화에 따른 DB 서버나 어플리케이션 서버의 부하가 상대적으로 적다. 그러나 이 방식을 적용하려면 암복호화 처리가 필요한 데이터양에 따라 다수의 Appliance 장비가 필요할 수 있어 Appliance 장비의 장애에 대한 대비 및 배치작업 수행 시 성능 등을 추가적으로 검토할 필요가 있다.

제4장

도입 시 고려사항

DB에 저장된 정보들은 DB내부의 인덱스, 내외부 어플리케이션 등과 밀접하게 상호 작용을 하므로 DB 암호화 후에도 이러한 시스템적 관계유지가 필요하다. 또한 DB서비스의 영속성을 위해 DB 암호화 후 기존 제약사항 이나 서비스의 안전성 유지가 무엇보다 중요하다. 이를 위한 DB 암호화 기술 도입 시 주요 고려사항은 암호화 대상, 암호 알고리즘, 암·복호화 범위, 암·복호화 키 관리, 암·복호화, 접근통제, 인증, 암호통신, 보안감사 등으로 구분할 수 있다.

1. 암호화 대상

- 법·규정 등에서 정의한 데이터를 포함한 개인정보를 암호화 대상으로 고려

암호화 대상은 국내 법·규정 등에서 규정한 개인정보 및 그 외 중요 데이터를 우선적으로 선정한다. 각 법률 및 규정에서 명시한 DB 암호화 대상은 비밀번호(패스워드), 고유식별정보[4](주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등), 신용카드번호, 계좌번호, 거래로그, 바이오정보(생체정보) 등이 있다. 정보의 특성에 따라 암호화 방식을 다르게 하도록 규정하고 있으며, 각 특성에 맞는 암호화 알고리즘으로 DB 암호화 기술을 적용해야한다. 각 법률 및 규정에서 정의하는 암호화 대상 및 방식은 다음 [표 10]과 같다.

4) 고유식별정보 : 「주민등록법」 제7조제3항에 따른 주민등록번호, 「여권법」 제7조제1항제1호에 따른 여권번호, 「도로교통법」 제80조에 따른 운전면허의 면허번호, 「출입국관리법」 제31조제4항에 따른 외국인등록번호

[표 10] DB 암호화 대상 및 암호화 방식

구분	대상	암호화 방식
공통	비밀번호(패스워드)	일방향 암호화 저장
개인정보보호법	여권번호	안전한 암호알고리즘으로 암호화하여 저장
	운전면허번호	
	외국인등록번호	
	주민등록번호	
	바이오정보	
정보통신망법	주민등록번호	안전한 암호알고리즘으로 암호화하여 저장
	신용카드번호, 계좌번호	
	바이오정보	일방향 암호화 저장
전자금융감독규정	거래로그	암호화하여 저장
신용정보업감독규정	생체정보	일방향 암호화 저장

원칙적으로, 금융회사에서는 개인신용정보는 신용정보법 및 관련 고시에 따라, 그 밖의 개인정보는 개인정보보호법 및 관련 고시에 따라 필요한 조치를 취해야 한다. 다만, 고유식별정보의 암호화는 개인정보보호법에서 특별히 정하는 의무사항이므로 금융회사가 업무상 수집·관리하는 모든 개인(신용)정보 전반에 대하여 적용됨을 유의하여야 한다.

개인정보보호법 상에서는 정보통신망을 통하여 개인정보를 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에 암호화하도록 규정하며, 인터넷구간 및 DMZ구간과 내부망으로 구분하여 내부망은 개인정보 영향평가(공공기관) 또는 위험도 분석결과[5]에 따라 DB 암호화 적용 여부와 적용범위를 정하여 시행가능하나, 인터넷 구간 및 DMZ구간에 개인정보를 저장하는 경우 위험도 분석과 관계없이 DB 암호화를 적용하도록 하고 있다.

5) 상세 내용에 대해서는 '[붙임 2] 관련 법률 및 규정' 참고

고유식별정보 중 주민등록번호(2016년 1월 1일부터 시행)는 영향평가 또는 위험도 분석결과와 무관하게 암호화 처리해야 하며, 영향평가 또는 위험도 분석 후 내부망에 DB 암호화를 적용할 경우, 송·수신되는 내부자 및 이용자의 비밀번호 또는 바이오정보는 암호화해야 한다. 그 외의 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있다. 전용선을 이용하여 개인정보를 송·수신할 경우 암호화 적용이 필수적이진 않지만 내부사용자에 의한 개인정보 유출에 대비하기 위해선 암호화 기술 적용을 고려하여야 한다.

2. 암호 알고리즘

- 표준화된 암호 알고리즘을 사용
- 안전성이 검증된 암호 모듈 사용 및 안전한 운영모드 적용

DB 암호화를 위해 사용하는 암호 알고리즘 및 키 길이 선택 시 보안강도[6], 안전성 유지기간 등에 따라 성능과 보안성의 차이가 존재할 수 있다. 암호화 대상 DB의 용도 및 연계시스템 간의 관계, 특히 DB 암호화 시스템의 운영 기간 등을 고려하여 보안강도 및 암호 알고리즘의 안전성 유지기간을 선택하여야 한다.

6) 보안강도 : 암호 알고리즘이나 시스템의 암·복호화 키 또는 해쉬함수의 취약성을 찾아내는데 소요되는 작업량을 수치화한 것으로 80, 112, 192 ,256비트로 정의되어 있으며, 80비트의 보안강도란 2^{80}번의 계산을 해야 암·복호화 키 또는 암호 알고리즘의 취약성을 찾아낼 수 있음을 의미

만약 112비트 보안강도의 암호 알고리즘을 적용을 고려할 경우, 2030년 이후에는 112비트 보안강도의 암호 알고리즘이 안전하지 않으므로 2030년 이후까지 사용하는 것을 고려한다면 더 높은 보안강도의 알고리즘을 선택하여야 한다. 다음 [표 11]은 암호 알고리즘의 보안강도 및 안전성 유지기간 등을 나타낸다.

[표 11] 암호 알고리즘 보안강도 비교표[7)]

보안강도	양방향 알고리즘 (대칭키 암호)	일방향 알고리즘 (해쉬함수)	암호 알고리즘 안전성 유지기간
80비트	80	80	2010년까지
112비트	112	112	2011년에서 2030년까지 (최대 20년)
128비트	128	128	2030년 이후
192비트	192	192	
256비트	256	256	

DB의 중요 데이터를 암호화하는데 적용되는 암호 알고리즘은 크게 일방향 알고리즘과 양방향 알고리즘이 있다. 일방향 알고리즘은 임의 길이의 정보를 입력으로 받아 고정된 길이의 암호문(해쉬값)을 출력하는 암호기술로 암호화된 정보는 복호화가 불가능한 특징을 가지고 있으며, 일반적으로 비밀번호 등을 암호화 할 때 사용된다. 일방향 알고리즘은 각 국가별 암호연구기관에서 다음 [표 12]의 알고리즘을 권고하고 있으며, [표11]의 암호 알고리즘 보안강도에 따른 안전성 유지 기간을 고려했을 때 112비트 이상의 알고리즘을 사용하여야 한다.

7) 암호 알고리즘 및 키 길이 이용 안내서, 한국인터넷진흥원, 2013

[표 12] 국내외 권고 일방향 알고리즘 및 보안강도

보안강도	NIST(미국) (2012)	CRYPTREC(일본) (2011)	ECRYPT(유럽) (2011)	국내 (2012)
80비트 이상	SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256 SHA-384/512 RIPEMD-160	SHA-1 SHA-224/256 SHA-384/512 RIPEMD-128/160 Whirlpool	HAS-160 SHA-1 SHA-224/256 SHA-384/512
112비트 이상	SHA-224/256 SHA-384/512	SHA-256 SHA-384/512	SHA-224/256 SHA-384/512 Whirlpool	SHA-224/256 SHA-384/512
128비트 이상	SHA-256 SHA-384/512	SHA-256 SHA-384/512	SHA-256 SHA-384/512 Whirlpool	SHA-256 SHA-384/512
192비트 이상	SHA-384/512	SHA-384/512	SHA-384/512 Whirlpool	SHA-384/512
256비트 이상	SHA-512	SHA-512	SHA-512	SHA-512

일방향 알고리즘 적용 시 암호화 값에 대한 사전 공격, 무작위 대입 공격 등을 대비하기 위해 Salt라는 비밀값을 추가할 수 있다. Salt는 동일한 평문 값인 경우에도, 암호화된 결과값을 다르게 만들어 비밀번호 노출 위협을 막을 수 있다. Salt는 암호화하는 데이터와 따로 분리하여 저장하여야 하며, 서버 프로그램 노출에 따른 Salt 값의 노출 위험을 막기 위해, 서버 프로그램은 Salt를 외부에서 호출하여 사용하는 형태로 구현하는 것이 적합하다.

주민등록번호 등의 개인정보 암호화 시 사용되는 양방향 알고리즘은 보안강도에 따라 112비트 이상 알고리즘을 적용하여야 하며, 각 국가별 암호 연구기관에서 다음 [표 13]과 같이 권고하고 있다.

[표 13] 국내외 권고 양방향 알고리즘 및 보안강도

보안강도	NIST(미국) (2012)	CRYPTREC(일본) (2011)	ECRYPT(유럽) (2011)	국내 (2012)
80비트 이상	AES-128/192/256 2TDEA* 3TDEA**	AES-128/192/256 3TDEA Camellia-128/192 /256 MISTY1	AES-128/192/256 2TDEA 3TDEA KASUMI Blowfish	SEED HIGHT ARIA-128/192/ 256
112비트 이상	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192 /256 MISTY1	AES-128/192/256 3TDEA KASUMI Blowfish	SEED HIGHT ARIA-128/192/ 256
128비트 이상	AES-128/192/256	AES-128/192/256 Camellia-128/192 /256 MISTY1	AES-128/192/256 KASUMI Blowfish	SEED HIGHT ARIA-128/192/ 256
192비트 이상	AES-192/256	AES-192/256 Camellia-192/256	AES-192/256 Blowfish	ARIA-192/256
256비트 이상	AES-256	AES-256 Camellia-256	AES-256 Blowfish	ARIA-256

* 2TDEA : 두 개의 키가 다른 TDEA(Triple Data Encyption Algorithm)

** 3TDEA : 세 개의 키가 다른 TDEA

DB의 데이터를 암호화하기 위해 안전성이 검증되지 않은 암호 모듈을 사용하거나, 적합하지 않은 운영모드를 사용하는 경우 암호문이

해독될 수 있다. 운영모드란, 입·출력값의 데이터 크기가 고정되어 있는 암호 알고리즘을 임의의 크기를 갖는 데이터에 적용할 때, 암호 알고리즘의 특성으로 인해 생긴 일정 크기의 출력값 간에 연관성을 주는 방식이다. 이는 기본 블록 단위 이상의 크기를 갖는 데이터의 암호화에 영향을 주는 것이 목적이며, 해시함수의 Salt와 같이 Initial Vector[8](이하 'IV')를 추가하여 출력 값으로 부터 입력 값을 유추하기 어렵게 만들 수 있다.

현재 국내외에서 권고되는 운영모드로는 ECB[9], CBC[10], CFB[11], OFB[12], CTR[13] 등이 있다. ECB운영모드는 같은 평문에 동일한 암호문이 생성되는 취약성으로 인해 암호문을 통해 암·복호화 키를 추측할 수 있기 때문에 사용이 제한되고 있다. 그러므로 유추로 인한 위험을 없애기 위해 IV를 사용하는 CBC, CFB, OFB 모드를 적용해야 한다. 단, IV를 사용하여 암호화 하는 경우에 고정된 IV를 사용하지 않도록 주의할 필요가 있다.

DB의 특성상 테이블끼리 Join 검색이 이루어지거나 FK(Foreign Key-외래키)로 참조되는 경우에는 IV사용이 제한적이므로 이럴 경우에는 유추 위험이 없는 CBC, CTR 모드를 사용하는 것이 적합하다.

---

8) Initial Vector : 초기화 벡터, 데이터 암호화를 위한 비밀 키와 함께 사용할 수 있는 임의의 숫자

9) ECB : 전자 코드북(electronic codebook, ECB)모드는 블록암호 운용 방식 중 가장 간단한 구조를 가지며, 메시지를 여러 블록으로 나누어 각각 암호화하는 방식

10) CBC : 암호 블록 체인(cipher-block chaining, CBC) 방식은 1976년 IBM에 의해 개발됨. 각 블록은 암호화되기 전에 이전 블록의 암호화 결과와 XOR되며, 첫 블록의 경우에는 Initial Vector가 사용됨. Initial Vector가 같은 경우 출력 결과가 항상 같기 때문에, 매 암호화마다 다른 Initial Vector를 사용해야 함

11) CFB : 암호 피드백(cipher feedback, CFB) 모드는 CBC의 변형으로, 블록 암호를 자기 동기 스트림 암호로 변환

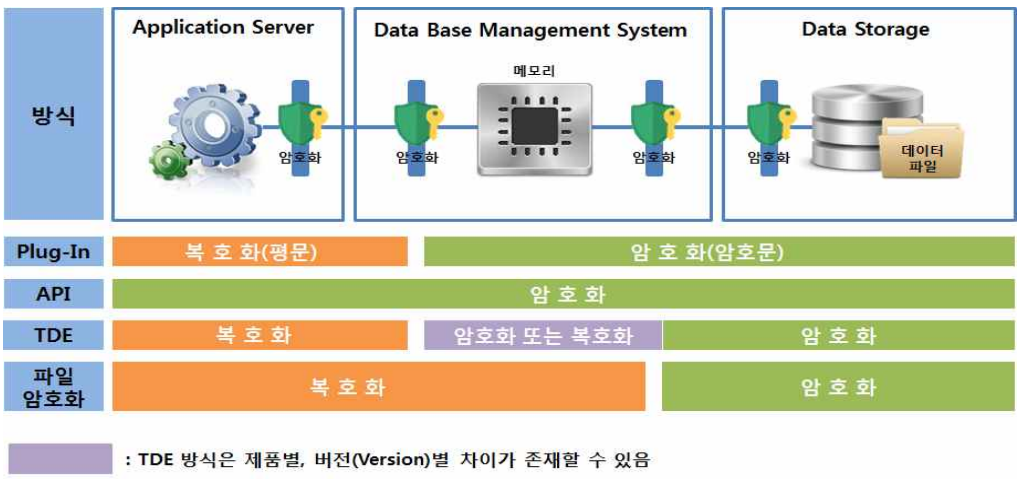
12) OFB : 출력 피드백(output feedback, OFB)모드는 블록 암호를 동기식 스트림 암호로 변환

13) CTR : 카운터(Counter, CTR) 모드는 블록 암호를 스트림 암호로 변환하는 구조로, 각 블록마다 현재 블록이 몇 번째인지 값을 얻어, 그 숫자와 nonce를 결합하여 블록 암호의 입력으로 사용

3. 암·복호화 범위

- 암·복호화 처리 시점 고려
- 데이터 특성 및 활용도 고려

DB 암호화 기술은 각 방식 특성(암호화 또는 복호화 처리되는 시점 등)에 기반하여 데이터의 암호화 또는 복호화의 범위(데이터가 암호문 또는 평문으로 조회 가능한 범위)가 다르며, 데이터의 특성 및 활용도에 따라 적합한 기술을 적용하여야 한다. 예를 들어 Plug-In 방식의 경우, DB 서버 내에 암·복호화 모듈을 설치하여 암·복호화를 수행하기 때문에, 스토리지 및 DB 서버 상에서는 데이터가 암호화된 형태로 존재하나, 데이터를 활용하기 위해 어플리케이션 서버로 데이터를 전송할 경우에는 데이터가 DB 서버 내에서 복호화 되어 어플리케이션 서버로 전송된다. 다음 (그림 8)은 각 방식별로 암·복호화 범위를 나타낸다.



(그림 8) 방식별 암·복호화 범위

4. 암·복호화 키 관리

- 암·복호화 키의 생성은 검증된 난수발생기를 사용하고 안전성이 검증된 표준 알고리즘을 사용하여 생성
- 키 분배 시에도 암호화 등을 통해 보안성 유지
- 암·복호화 키 및 마스터키는 암호화되어 DB서버 이외의 별도 저장소에 저장
- 암·복호화키, 마스터키 등 인가된 사용자만 접근 가능, 공유 메모리에 로드되어 있는 암·복호화 키는 평문으로 존재 불가
- 암·복호화키 백업 및 복구 절차 수립 및 이행
- 일정 기간마다 키 교체 수행
- 암·복호화키 폐기 절차 수립

암호화 시 키가 노출되면 암호화된 데이터를 복호화 할 수 있기 때문에 키를 안전하게 관리하는 것은 매우 중요하다. DB의 암·복호화를 위해 사용되는 암·복호화 키의 종류는 암·복호화 키와 마스터 키 두 가지로 크게 나눌 수 있는데, 암·복호화 키는 DB 내 데이터의 암·복호화를 위해 사용 되며, 마스터 키는 암·복호화 키를 암호화하기 위해 사용 된다.

암호화된 데이터 유출 시 이를 해독할 수 있는 암·복호화 키는 암호화 대상이 되는 데이터만큼이나 중요한 정보이다. 아무리 강력한 암호를 사용한다 할지라도 메모리 덤프 공격 등을 통해 암호화 키 정보가 외부에 노출되면 해당 키로 암호화된 데이터는 평문으로 저장된 것과 마찬가지이므로 사용되는 키는 공유 메모리에 로드될 경우 평문으로 존재하지 않아야 한다. 암·복호화 키는 마스터키를 사용하여 암호화하고, 실제

암·복호화 키를 사용하는 시점에만 임시로 복호화하여 사용하여야 한다. 마스터키 또한 유출이 불가능하도록 하거나 유출이 되어도 활용할 수 없도록 생성부터 폐기까지 안전하게 관리되어야 한다. (그림 9)는 단계별 키 관리 절차를 나타낸다.

(그림 9) 키 관리 절차

가. 키 생성

암·복호화 키를 생성하기 이전에 보안을 위해 유효기간을 설정할 필요가 있다. 유효기간은 사용자 또는 관리자가 암·복호화 키를 사용할 수 있도록 허용된 기간과 사용기간이 완료된 이후라도 추후 복호화 과정에서 해당 암·복호화 키를 사용하도록 허용된 기간으로 구분할 수 있는데 NIST(National Institute of Standards and Technology)의 키 관리 권고안[14]에서는 해당 유효기간을 각각 최대 2년, 최대 5년으로 설정하도록 제시하였다.

암·복호화 키를 생성하기 위해서는 다음의 두 가지를 고려하여야 한다. 첫째, 암·복호화 키 생성시 안전한 난수 발생기를 이용하여야

14) NIST Special Publication 800-57 Recommendation for Key Management-Part 1: General(Revision 3)

하며 둘째, 사용자 입력으로부터 유도되는 암·복호화 키 또한 안정성이 검증된 알고리즘을 사용하여 생성하여야 한다.

각각의 업무를 처리하기 위해 시스템들은 DB의 암호화된 데이터를 복호화하는 키를 사용할 것이고 하나의 암·복호화 키로 구성된 데이터는 암·복호화 키가 유출되면 기밀성이 유지되지 않아 암호화의 의미를 잃게 된다. 그러므로 업무 범위나 시스템의 역할 등을 고려하여 암·복호화 키를 테이블 또는 컬럼에 따라 다르게 생성하여 사용한다면 암·복호화 키에 대한 보안성을 강화하고, 개별적으로 키 교환이나 폐기를 처리할 수 있어 하나의 암·복호화 키를 사용하여 전체를 암호화 하는 방식보다 유연한 세부적 정책 설정이 가능하다. 다수의 암·복호화 키로 분리하여 보안성을 강화하여도 해당 암·복호화 키에 대한 접근제어 정책이 반드시 수반되어야 한다.

나. 키 분배

키 분배라 함은 암·복호화 키를 생성한 후에 이를 안전하게 분배하는 것을 말한다. 키 분배 시에도 암호화 등의 방법을 통하여 보안성을 유지하여야 한다. 키 관리 서버가 별도로 존재하는 경우에도 생성된 암·복호화 키 분배 및 정책 배포를 위해 암호화 등의 방법을 통하여 암·복호화 키의 외부 노출을 차단하여야 한다.

다. 키 저장

암·복호화 키를 저장하는 방법 중 쉬운 방법은 제한된 테이블이나 파일에 암·복호화 키를 저장하는 것이다. 이러한 방법은 DB 관리자가 접근권한을 가지고 있다면, 데이터를 임의로 복호화 할 수 있고 해당 테이블이나 파일이 함께 유출된 경우, 데이터를 해독할 수 있어 내·외부 위협에 노출될 가능성이 있다. 따라서 DBMS 내부에 암·복호화 키를

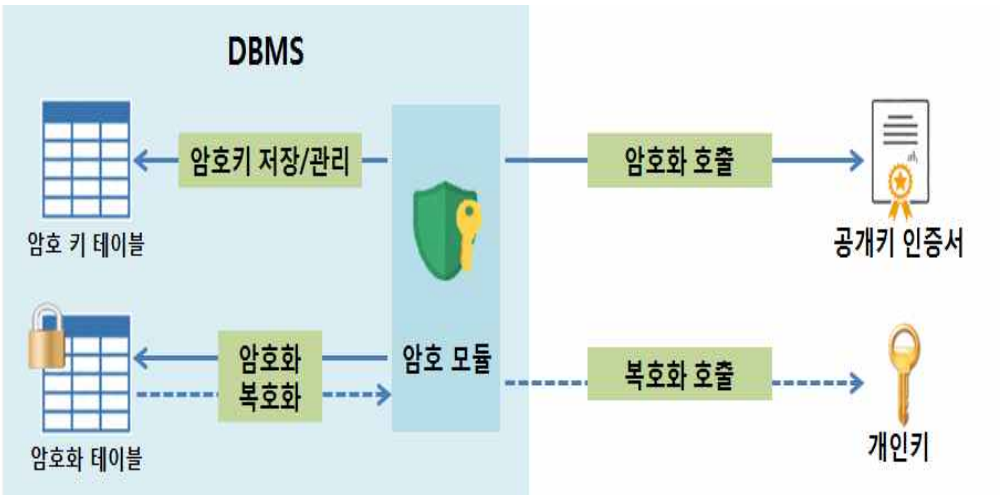
저장하기 보다는 DBMS와 분리된 별도의 키 관리 서버, HSM 장비 등을 통해 암호화 하여 저장하는 것을 고려하여야 한다. 별도에 장비에 암·복호화 키를 분리하여 관리할 시에도 시스템에 대한 접근통제 및 인증 정책이 수반되어야 하며, 해당 장비는 물리적으로 안전하게 보호해야 할 것이다.

라. 키 사용

암·복호화 키에 대한 접근제어 정책이 없다면, 개발자부터 DB 관리자까지 누구나 해당 암·복호화 키를 접근할 수 있게 되므로 기본적으로 DB 관리자는 암호화된 데이터를 직접 조회하거나 데이터 및 암·복호화 키에 대한 접근 권한을 가질 수 없도록 DB 관리자와 보안 관리자의 권한을 분리하여야 한다. 또한, 하나의 테이블에 존재하는 서로 다른 컬럼이라 하더라도 사용자를 식별하여 복호화 할 수 있도록 암·복호화 키 분리 정책 및 복호화의 권한 제한을 설정할 필요가 있다. 복호화 권한 없는 사용자에게는 암호화된 데이터나 부분 암호화(Maskimg 등) 데이터를 전송하여야 한다.

공유 메모리에 로드된 암·복호화 키도 평문으로 저장해서는 안 되며, 마스터키와 같이 키를 암호화하는 핵심보안 매개변수도 안전하게 관리되어야 한다. 암·복호화 키와 마찬가지로 접근 및 변경은 인가된 사용자에게만 허가 되어야 한다.

또한 (그림 10) 처럼 공개키를 이용하여 암·복호화 키를 암호화하는 등 암·복호화 키를 안전하게 사용 할 수 있는 방안을 마련해야 한다.



(그림 10) 공개키를 이용한 암·복호화 키 보호

마. 키 백업 및 복구

암·복호화 키 및 패스워드의 분실 또는 훼손, 키 관리자의 퇴사 등으로 암·복호화 키와 패스워드를 알 수 없는 경우에 대비하여 암·복호화 키를 복구하기 위한 백업 절차를 수립하여야 한다. 또한 암·복호화 키 분실 시 데이터 복호화가 불가능하므로 분실, 훼손, 파괴 등의 경우에 대비하여 키를 복구하기 위한 방안도 마련해야 한다.

암·복호화 키는 백업 정책에 따라 주기적으로 백업되어야 하며, 백업된 키 정보는 암호화 하여 저장해야 한다. 또한 키 백업에 사용한 암·복호화 키는 별도로 관리되어야 한다.

암호화된 데이터를 백업하는 경우 해당 데이터를 암호화 한 암·복호화 키도 백업해야 향후 백업된 암호화 데이터를 복호화 하여 이용할 수 있다.

바. 키 교체

암·복호화 키는 기업 내부 정책에 부합하는 기간마다 교체하여 보안성을 유지하도록 해야 한다. 키를 교체하기 전 기존 키로 암호화된 데이터는 복호화 후 새로운 키로 다시 암호화하여야 한다.

※ 암·복호화 키가 노출된 경우 키 교체 등 보안 방안 필요

- 신규 데이터 - 변경된 키를 사용하여 암호화
- 기존 암호문 - 마이그레이션 작업을 통하여 신규 암호문으로 변경

사. 키 폐기

암·복호화 키는 여러 가지 이유로 폐기 될 수 있다. 예를 들어, 암·복호화 키 또는 마스터키를 분실하거나 키의 비밀성이 깨진 경우 등에 대비하여 키를 폐기하기 위한 절차 및 방법을 수립함으로써 허가된 관리자가 절차에 따라 폐기할 수 있도록 하여야 한다.

암·복호화 키를 폐기하게 되면 기존에 암호화 된 데이터는 더 이상 복호화 할 수 없으므로, 암·복호화 키 폐기 전 복호화 후 폐기하여야 한다. 또한 제품 종료 후 메모리에 로드된 암·복호화 키와 핵심보안 매개변수는 모두 제거하여 유추할 수 없도록 해야 한다.

5. 암·복호화

- 암호화 컬럼에 대한 인덱스 검색 지원
- 인덱스 컬럼 암호화를 통한 인덱스 보호.
- 부분암호화 기술 적용 고려
- 암호화 및 데이터 저장 공간 확보
- 데이터 암호화 후 원본 데이터 삭제 필요
- 암호화 후 성능 부하 정도 파악 및 감소 방안, 전략 필요

데이터의 분실, 도난, 유출 등의 위협에 대응하여 보안성을 보장하기 위해서는 인가된 사용자만이 안전성이 검증된 알고리즘을 사용하여 암호화하여야 한다.

가. 인덱스 검색

암호화 컬럼의 데이터 타입에 따라 인덱스의 컬럼 값이 그대로 노출되는 경우가 있기 때문에 인덱스를 통한 원본 데이터의 유출 위협에 대응하기 위해서는 인덱스 컬럼에 대한 암호화를 수행하여야 한다.

그러나 인덱스 컬럼에 대해 암호화를 적용하면, 인덱스를 활용할 수 없어 부하 및 성능 저하가 발생할 수 있다. 이러한 경우는 별도의 다른 컬럼으로 유도하는 등 데이터 검색 속도 등을 향상시키기 위해 암호화 적용 후 해당 컬럼에 대해서 기존 인덱스를 유지할 수 있는 방안을 강구하는 것이 좋다.

나. 부분암호화

주민등록번호, 신용카드번호, 계좌번호 등 인덱스로 사용되는 데이터 전체를 암호화하게 되면 암호문을 통한 일치 검색은 가능하지만 범위 검색 시 성능 저하가 발생하여 원활한 서비스 제공 및 기존 환경과 동일한 수준의 가용성 보장이 어려울 수 있다. 이러한 경우 인덱스 컬럼의 보안성을 유지하며 가용성을 보장받기 위한 방안으로서 인덱스 컬럼에 부분 암호화 기술을 사용하여 최소한의 필수 정보만을 평문으로 유지하고 이외에 데이터는 암호화하여 검색 속도를 향상 시킬 수 있다.

부분 암호화 기술를 적용하면 암호화 후에도 인덱스를 통한 전방 일치 검색, 일치 검색, 범위 검색을 할 수 있다. 아래는 주민등록번호 및 신용카드번호의 부분 암호화에 대한 예시이다.

[주민등록번호]
- 생년월일과 성별(또는 외국인) 정보를 포함하고 있는 7자리를 제외한 뒷자리 6개 번호 이상을 암호화 (771111-1#.....&)

[신용카드 번호]
- 카드유형 정보(국내/VISA/MASTER 등)를 포함한 6자리를 제외한 뒷자리 10개 번호 이상을 암호화 (2222-20$.....^)

다. 데이터 저장 공간

암호화 솔루션을 설치하고 암호화 적용을 위해서는 설치 및 로그 파일 저장 공간과 암호화 작업 공간이 필요하다. 적용하는 암호화 방식 및 암호 모듈에 따라 데이터 사이즈가 증가하는 다양한 케이스가 존재할 수 있다.

- 작은 크기의 원본 데이터를 암호화 후 데이터 사이즈가 증가하여 DB 컬럼의 사이즈까지 조정해야 하는 경우
- 텍스트 블록을 이진데이터로 암호화한 경우 다시 텍스트 형태로 변환하여야 하기 때문에 사이즈가 변화하는 경우 등

일반적으로는 암호화 적용 시 생성되는 암호화 테이블은 원본 사이즈보다 커지게 되므로 원본 테이블 이상의 추가적인 저장 공간이 필요하다. 암호화 적용 도중 원복을 해야 하는 경우도 발생할 수 있으므로 Rollback Size 확보도 필요하다.

라. 원본 데이터 삭제

데이터 암호화 완료 후에는 원본 데이터 유출 방지를 위하여 원본 데이터는 모두 폐기 되어야 한다. 서비스가 진행 중인 DB와 백업 스토리지에 저장된 원본데이터가 그 대상이며, DB서버 내 디스크의 원본 데이터는 테이블의 컬럼 값 및 인덱스 정보까지 포함하여야 한다.

마. 성능

DB 암호화를 적용하면, 데이터 길이의 증가, 시스템 메모리 사용량 증가 등으로 인해 암호화 적용 전보다 성능이 저하된다. 이외에도 암호화 알고리즘의 종류와 키 길이에 따라 암/복호화 성능에 영향을 미칠 수 있고, 암호화 방식 및 서비스 특징에 따라서도 DB 암호화 적용 후 성능에 영향을 미치는 정도가 다를 수 있다. 그러므로 다양한 암호화 방식을 검토하여 부하를 감소시키기 위한 전략이 필요하다.

암호화 후의 성능저하를 방지하기 위한 다양한 방법 및 구성이 존재하므로 적합한 방법을 선택하여야 한다. 이러한 방법의 하나로 암호화 후 컬럼사이즈 증가에 따른 성능저하를 방지할 수 있는 형태보존함수(Format Preserving Encryption, 이하 FPE)를 사용하거나 암호화 데이터의 순서를 유지하여 암호화 후 발생하는 복호화 연산의 부담을 해결하는 순서유지 암호화함수(Order Preserving Encryption, 이하 OPE)를 사용하는 방법이 있다.

FPE는 주민등록번호, 신용카드번호 등에 대한 암호문이 평문과 같은 형태를 유지하도록 하는 암호화 방식으로 금융정보, 데이터 완전삭제, DB 보안에 활용될 수 있는 암호화 알고리즘이다. 현재 NIST[15]에는 FCEM[16], FFX[17], BPS[18], VEPE[19], CSPEM[20] 등 5가지 FPE 암호화 알고리즘이 제안되어 있으며, 국내에서는 FEA[21] 알고리즘이 제안되어 있다. 많은 전문가들이 보안성과 효율성 등의 검증을 계속적으로 진행 중이므로, 향후에는 DB 암호화 기술에 적용될 수 있을 것으로 예상된다.

OPE는 암호화를 적용하더라도 암호화된 데이터들이 원본 데이터와 동일한 순서로 정렬될 수 있도록 해주는 방법으로 암호화된 데이터에 대해서도 DB의 검색 색인을 용이하게 만들 수 있다는 장점이 있으나 암호문에서 '순서'라는 정보를 얻을 수 있고 이를 바탕으로 평문을 유추할 가능성이 있다. 예를 들어 ABCD의 암호문(A)과 CDEF의 암호문(B)을 안다면, 암호문(A)와 암호문(B) 사이에 정렬될 수 있는 암호문(C)는 ABCD와 CDEF의 사이에 있는

15) http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html
16) FCEM : Format Controlling Encryption Mode, U. Mattsson
17) FFX : Format-preserving Feistel-based Encryption Mode, M. Bellare, P. Rogaway, T. Spies
18) BPS : Format Preserving Encryption Proposal, E. Brier, T. Peyrin, J. Stern
19) VFPE : VISA Format Preserving Encryption, VISA USA
20) CSPEM : Character Set Preserving Encryption Mode, Gary S. Sarasin
21) FEA : Format-Preserving Encryption Algorithms, NSRI

어떤 값으로부터 만들어진 암호문임을 알 수 있다. 이렇듯 OPE는 어떤 수를 암호화한 값인지를 구분할 수 없는 비구별성(Indistinguishability)를 만족하지 못하기 때문에 검증받은 암호화 알고리즘을 함께 사용하거나 순서정보만을 한번 더 암호화 하는 등 OPE를 활용하여 DB 암호화로 인한 성능 영향을 감소시키기 위해서는 안전성을 보완해줄 보안장치 및 기술 적용이 필요하다.

6. 접근통제

- 일반 사용자(조회 등 업무 수행), DB 관리자, DB 운영자, 시스템 개발자, 시스템 운영자, 시스템 관리자, 보안 관리자 등의 권한 분리
- DB 보안 관리자의 승인 없이 암호화된 데이터에 대한 암·복호화 금지
- 사용자 보증을 위한 식별 및 인증 수행
- 인증 데이터는 안전한 방법으로 전송하고 재사용 위협을 고려

데이터 유출을 방지하기 위해 DB 암호화를 적용하지만 암호화 데이터, 암·복호화 키, 핵심보안 매개변수 등의 보안성 유지와 이들에 대한 내부 사용자의 불법적 접근을 방지하기 위해서는 접근통제 기능도 고려해야 한다. 접근통제에 대한 부분은 아래 [표 14]와 같이 법률 및 규정에서도 적용하도록 명시하고 있다.

[표 14] 접근통제 관련 법률[22)]

구분	내용
개인정보보호법	개인정보에 대한 접근 통제 및 접근 권한의 제한 조치를 하도록 함
정보통신망법	개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치를 설치·운영하도록 함
전자금융감독규정	전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제하도록 함

22) 상세 내용에 대해서는 '[붙임 2] 관련 법률 및 규정' 참고

가. 권한분리

DB에 접근하는 경우는 웹이나 어플리케이션 서버의 정형적인 접근[23], DB관리자 등에 의한 비정형적인 접근[24]으로 구분할 수 있는데, 접근 유형에 따라 사용자는 적합한 접근 권한을 부여 받아야 한다.

암호화가 적용된 데이터는 어플리케이션 프로그램(DB접속 프로그램, 사용할 수 있는 SQL 종류 등 통제), 접속자 IP 및 Port · MAC주소, 접속 기간·시간·요일, DB 사용자 계정 등에 의한 접근 통제 정책에 따라 인가되지 않은 사용자의 불법적인 접근을 통제하여야 한다.

또한 보안관리자, DB 관리자, 개발자 등의 권한을 명확히 분리하여야 한다. 특히 DB관리 권한과 접근통제 관리권한은 반드시 분리하여야 한다. 보안관리자(접근통제 관리)는 암·복호화 키 관리, 암호화 정책 등을 관리하되 DB에 접근할 수 없어야 하며, DB 관리자는 암호화된 상태의 DB는 관리하되 암·복호화 키에 대한 접근을 통제하여 DB의 내용을 복호화 할 수 없도록 한다. 개발자는 암·복호화 키에 접근하지 못하며 불필요한 DB 접근 권한을 갖지 않도록 하여 정보 유출 및 오·남용이 발생하지 않도록 고려하여야 한다.

나. 사용자 인증 및 식별

DB 사용자 계정 및 비밀번호가 노출 되면 해당 사용자에게 부여된 권한을 그대로 사용할 수 있기 때문에 식별 및 인증 과정을 통해 DB에 접근이 가능한 정당한 사용자임을 보증하여야 한다.

---

23) 정형적인 접근 : 특정 업무 수행을 위해 정기적으로 DB에 접속하여 반복적인 SQL 작업을 수행하는 것
24) 비정형적인 접근 : DB에 접속하여 데이터를 변경, 삭제 및 조회를 수행하는 것

사용자 인증은 일반 사용자 및 관리자 인증으로 나뉠 수 있다. 일반 사용자는 인증 실패 횟수 제한 등 계정 및 비밀번호 관리 정책에 따라 복잡도 수준을 결정하고, 관리자는 보안 정책 설정, 감사기록 관리 등의 보안 수준이 높은 업무를 수행하기 때문에 다양한 인증 방법 및 다단계 인증을 고려하여 인증 수준을 강화할 수 있다. 사용자를 식별하는 인증 방법은 크게 3가지로 구분할 수 있다.

① 지식기반 : 사용자가 가진 지식이나 알고 있는 정보를 확인하여 인증(ID/비밀번호등)
② 소유기반 : 소지한 인증수단을 이용하여 인증(보안카드, OTP 등)
③ 생체기반 : 사용자가 가진 특징을 이용하여 인증(지문, 홍채 등)

계정 및 비밀번호와 같은 인증데이터도 제3자에게 노출되거나 변경되지 않아야 하며, 인증데이터의 재사용 공격을 방지해야 한다.

7. 암호통신

- 암복호화 시스템 및 모듈 간의 통신 구간 보호

데이터 암복호화를 수행하는 시스템 및 모듈 간에 통신 구간을 통하여 데이터, 암·복호화 키, 정책 등의 중요 정보가 전송된다. 통신 구간이 보호되지 않을 경우 네트워크 도청으로 정보수집 및 분석이 가능하기 때문에 전송 데이터의 기밀성·무결성 유지를 위해 전송 구간에 대한 보안 수준을 보장하는 것은 중요하다. 물리적으로 분리된 모듈 구성인 경우 송·수신되는 통신 데이터는 SSL, IPSec 등을 사용할 수 있다.

8. 보안감사

- 정책 설정, 암복호화 키의 변경, 접근 및 작업(조회·수정·추가·삭제), 성능 변화 등에 대한 감사 데이터 생성
- 감사데이터는 인가된 관리자만이 접근 가능
- 인가된 사용자만 정책을 설정할 수 있도록 하여야 하며 암호화된 컬럼에 대해 비인가자의 암·복호화 차단
- 암·복호화 키, 정책 등 데이터에 대한 백업 및 복구

가. 보안감사

암호화 대상 컬럼에 대한 암·복호화 수행 및 정책 관리에 대한 행위를 추적하는 보안 감사 정책을 통해 개인정보 및 업무 활동상의 중요 정보 자산을 보호해야 한다. 보안 감사를 크게 분류하면 감사 수준에 따른 정보 기록과 감사 정보에 대한 보호의 측면으로 나눌 수 있다.

감사 수준에 따른 보안 감사를 통하여 암호화 정책 설정 및 변경 이력, 암·복호화 키의 변경 및 사용 이력, 접근 및 작업 내역, 성능 변화 등에 대한 기록이 가능하다.

- 정책 설정 및 변경 : 암호화 대상 DB등록, 백업 및 복구 내역 등
- 암·복호화 키의 변경(생성/폐기) 및 사용 이력
- 접근 및 작업 내역 : 암호화 대상(테이블, 컬럼 등)에 대한 접근내역과 비인가 사용자에 대한 통제 결과, 데이터 조회·수정·추가·삭제 내역
- 성능 변화 : 암/복호화 엔진의 성능(분당/처리속도, 암/복호화 처리량 등) 변화를 기록

특히 이벤트 주체, 암호화 대상, 접근 정보 및 시간, 작업 내역 등의 상세한 감사 기록은 감사 자료를 활용한 탐지 및 추적에 유용한 자료로서 활용이 가능하기 때문에 다양한 수준의 보안 감사는 중요 정보 자산의 보호를 위해 중요한 고려 사항이다.

감사 정보의 보호를 위하여 감사 데이터는 인가된 관리자만이 접근할 수 있도록 하고 감사 관리자는 감사 데이터의 조회 및 모니터링만 가능하도록 하여 관리자 권한의 남용을 방지하여야 하며, 감사 데이터의 유출 및 위·변조가 발생하지 않도록 조치하여야 한다. 추가적으로 감사 정보 저장 시 저장소가 포화상태가 되어 정보 손실이 발생하지 않도록 정기적으로 저장소의 상태를 체크하여야 하고, 보안 수준이 높은 감사 정보는 보안 관리자에게 통보하여 다양한 위협에 대비하여야 한다.

나. 보안관리

암·복호화 키와 정책은 안전하게 관리되지 않으면 다양한 공격에 노출될 수 있다. 암·복호화 키와 정책이 노출되면 암호화된 데이터의 복호화가 가능하고 암·복호화 키 및 정책의 파괴, 유출, 변조 등의 다양한 위협이 발생할 수 있다.

암·복호화 키 및 저장소의 보호를 위하여 마스터키, 암·복호화 키 및 정책은 인가된 관리자만이 생성·변경·삭제할 수 있도록 하여야 한다. DB 서버에 암·복호화 키와 정책을 저장하는 경우에는 반드시 암호화 시켜 저장하여야 하며, 암·복호화 키의 사용을 위해 복호화하는 경우에는 (여러 차례에 걸쳐 서로 다른 키로 암호화 하였더라도) 최종적으로는 패스워드 입력에 의해 복호화 되거나 공개키 기반의 안전한 구조에 의해 복호화 되어야 한다.

암·복호화 키 및 정책의 복구는 인가된 관리자에 의하여 수행되어야 하며 암복호화키가 생성·변경되면 해당 암·복호화 키의 백업을 수행하는 등 안전하게 백업 및 복구가 되도록 절차를 마련하여야 한다.

제5장

구축 방안

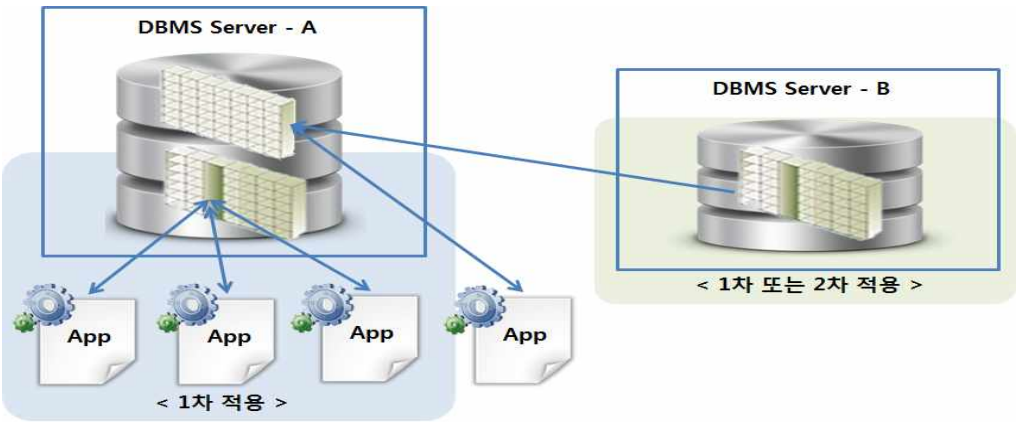
1. 구축전략

가. 단계별 적용

DB 암호화 기술 적용을 위해 단계별로 적용 단위를 나눌 수 있다면 효과적으로 구축할 수 있다. 적용단위를 구분하는데 있어 고려해야할 사항은 업무프로그램 단위와 적용 시점이다. DB 암호화를 하게 되면 암호화된 테이블별로 관련된 SQL들이 영향을 받기 때문에 업무프로그램 단위로 관계된 테이블들을 1차 적용 단위로 정하고, 추가적으로 테이블들끼리 또는 DBMS끼리 연결되어 있다는 점을 고려하여 일시에 적용할 것인지 또는 그 이후 적용 단위로 적용할 것인지를 결정해야 한다.

이 때 업무프로그램의 영향을 세밀히 파악할 수 있어야 하며, 사전에 분석된 ERD(Entity Relation Diagram)에 따라 암호화할 테이블과 관련된 모든 SQL들이 포함된 업무프로그램과 DB Link 등을 통한 타 DB와의 데이터 연계 부분을 체크해야 한다.

아래 (그림 11)와 같이 DB 암호화 구축 일정을 계획할 때는 먼저 업무단위로 분류하여 관계된 테이블들을 암호화 대상으로 선정할 수 있으며, 다른 DB와 DB Link 등으로 연계된 경우는 운영 측면과 성능 측면에서 함께 구축 대상에 포함할 수도 있다.



(그림 11) DB 암호화 단계별 적용 예

상대적으로 SQL에 영향을 적게 받는 블록암호화 방식은 데이터 용량에 따라 암호화 작업이 소요되는 시간과 암호화 작업에 할당된 시간을 파악하여 적용단위를 조정하여야 한다. 만약 데이터 용량에 따른 암호화 소요시간이 8시간으로 산정되었고, 작업에 할당된 시간이 4시간인 경우, 적용단위를 데이터 크기에 따라 2차에 걸쳐 적용하는 방안으로 진행할 수 있다.

나. Risk 관리

DB 암호화 기술은 대단위의 데이터를 암호화하고 기존의 평문상태의 테이블을 삭제한 후에야 비로소 DB 암호화 기술이 적용된 암호화 데이터 운영이 가능하다. 그러므로 암호화 구축을 이행한 후에 운영에 대해 사전에 충분히 검증하는 절차가 매우 중요하다.

- 컬럼암호화 방식 : Test DB에서 SQL 테스트 미흡으로 인해 발생할 수 있는 문제점들을 충분히 검증하는 절차가 필요
- 블록암호화 방식 : 주요 온라인 업무에 대한 부하테스트, 최대 용량의 배치 작업에 대한 테스트 등 사전 검증이 필요

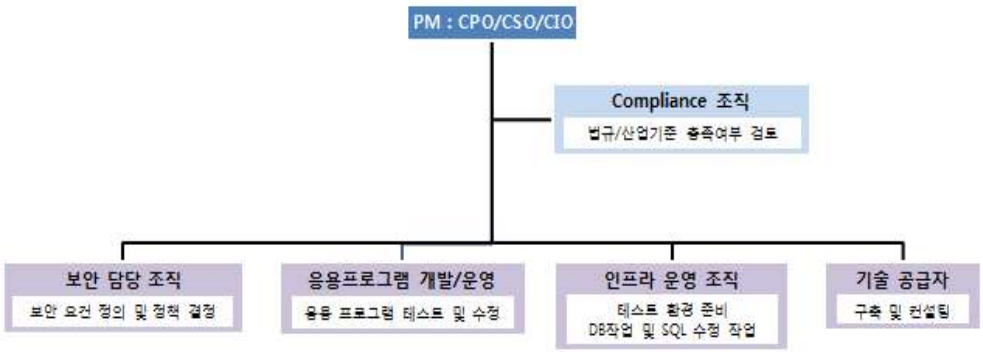
DB 암호화 구축 시 운영 DB에 적용 후 문제가 발생하지 않도록 암호화 구축을 이행한 이후에 충분한 테스트를 통해 리스크를 최소화하여야 하지만, 혹시라도 검증 미비로 말미암아 발생할 수 있는 사태에 대한 대비책으로 즉각적인 원복 체계 등을 강구해야 한다.

2. 구축 체계 및 절차

가. 역할 및 책임

DB 암호화는 단순한 보안기술이 아닌 DB와 관련성이 매우 큰 특성을 지니고 있어 보안 담당, 기술 공급자, 인프라 운영, 어플리케이션 운영 등의 관련 조직이 목적과 필요성에 전적으로 공감하고 적극적인 협조가 필수적이다.

다음 (그림 12)는 다양한 IT환경과 컴플라이언스 대응 등을 고려하여 DB 암호화 구축을 위한 조직의 체계 구성의 예이다.



(그림 12) DB 암호화 구축 시 조직 구성 예

DB 암호화에 따른 관련 조직들 간의 역할과 책임은 기본적으로 다음의 [표 15]와 같이 정의 할 수 있다.

[표 15] 관련 조직의 역할과 책임 예

조직	구분	역할	책임
보안 담당 조직	공통	-암호화 대상 컬럼 및 적용 알고리즘 선정 -보안 및 권한통제 정책 결정	-각 파트에 대한 협조유도 및 통제 -관련 규정에 따른 적용 대상 정보의 규정 및 알고리즘에 대한 책임 -권한통제 정책설정에 대한 책임
기술 공급자	공통	-암호화 영향도 분석 가이드 (부하 이슈 유형 및 해결 방안 안내) -개발/테스트 지원 -성능 제고 및 효율적인 구축 방안 가이드 -권한통제 정책 결정시 가이드 -제품 설치 및 대상 정보 암호화 작업 -제품의 운영 지침 교육	-제품의 보안성 및 안정성 책임 -중요 보안요소 및 위협에 대한 고지 -제품 운영에 필요한 정보 전달
인프라 운영 (시스템 & DBA)	컬럼 암호화	-암호화대상 테이블의 상세 정보 조사 -필요한 테스트 환경 및 H/W 자원 준비 -영향도 평가 분석 및 주관 -운영 DB 적용 시 관련 서비스의 중단/재기동 실시	-H/W 준비 및 DB 정보의 정확한 파악 및 보고 -어플리케이션 소스를 제외한 모든 DB 내·외부의 SQL문 중 암호화 테이블과 관련있는 SQL의 조사/테스트/수정/관리 -수정이 필요한 SQL문들을 제품 공급사의 조언대로 수정/테스트 하여 어플리케이션 운영팀에 전달 -운영 DB 적용 시 관련 서비스의 중단/재기동을 위한 인프라 운영체계 마련(사전 공지 등 포함)

인프라 운영 (시스템 & DBA)	블록 암호화	-암호화대상 테이블의 상세 정보 조사 -필요한 테스트 환경 및 H/W 자원 준비 -운영 DB 적용 시 관련 서비스의 중단/재기동 실시	-H/W 준비 및 DB 정보의 정확한 파악 및 보고 -운영 DB 적용 시 관련 서비스의 중단/재기동을 위한 인프라 운영체계 마련 (사전 공지 등 포함)
응용 프로그램 개발/ 운영	컬럼 암호화	-암호화대상 테이블 관련 SQL문을 포함한 소스 조사 -영향도 평가 지원 (암호화 후, 조사된 모든 SQL문을 실행하여 결과 추출) -추출된 결과 중, 성능이슈 또는 실행상의 문제점 등으로 인해 수정을 요하는 SQL문 제출 -인프라 운영팀에서 수정된 SQL문을 소스에 반영 -반영된 버전의 어플리케이션을 운영 DB 암호화 시에 어플리케이션 서버에 반영	-어플리케이션 내의 암호화 테이블 관련 SQL문의 전수 조사 -전수 테스트 -어플리케이션 소스에 반영 및 관리책임 -운영 DB 적용 시에 인프라 운영팀의 요청에 따라 해당 서비스의 운영 업무 수행
	블록 암호화	-영향도 평가 지원 -서비스 운영	-OLTP/Batch 별로 주요 업무를 선정하여 암호화 전후 성능 측정을 통해 영향도 산정 -운영DB 적용 시에 필요 절차에 따라 서비스 재기동 등의 운영 업무 수행

나. 구축 절차

DB 암호화 구축은 다음의 (그림 13)과 같이 사전협의, 사전 영향도 분석, 테스트 검증, 구축 및 안정화의 절차로 이루어진다.

(그림 13) DB 암호화 구축 절차

3. 단계별 구축 방안

가. 사전 협의

DB 암호화를 구축하기에 앞서 참여하는 모든 조직은 사전에 충분히 필요한 정보를 공유할 목적으로 본 단계를 수행해야 한다. 또한 DB 암호화 방식에 따른 암호화 대상, 적용 환경, 보안 등 사전에 필요한 사항에 대해 협의하여야 한다.

※ '[붙임 1] 사전 협의 시 고려사항'을 참고

나. 영향도 분석

암호화 적용 이전에 운영서버에 대한 모니터링을 통해 어플리케이션과 DBMS의 영향도를 분석하는 단계이다. DB 암호화 구축 단계에서 테스트/검증 단계와 함께 가장 중요한 단계로 DB 암호화 기술을 선정하거나 도입할 때에 반드시 검토되어야 한다.

운영시스템에 암호화를 적용하기 전에 암호화 대상 추출, 암호화 관련 SQL 쿼리 등을 미리 추출하여 테스트 시스템에서 성능 테스트를 수행하는 등 암호화 사전 진단을 수행하는 것이 필요하다. 전체적으로 DBMS 분석, 응용 프로그램 분석의 단계를 수행하여 암호화 이후 성능 및 시스템 리소스, Object 변화 등의 영향도를 분석한다.

① 암호화 대상 추출

전체 DBMS의 테이블과 컬럼을 검색하여 암호화 대상이 되는 데이터 컬럼을 추출한다.

예시) 추출된 컬럼

No	소유자 이름	테이블 이름	컬럼 이름	데이터 타입	길이	암호화시 길이 변경	개인정보타입	관련쿼리 개수	접근빈도
1	HRMDB	ADMONIT	DETAIL_ADDR	VARCHAR2	300	304		2	5
2	HRMDB	ADMONITIONREG	TEL	VARCHAR2	30	32		2	5
3	HRMDB	EXPERTMANAGER	DETAIL_ADDR	VARCHAR2	300	304		7	100
4	HRMDB	EXPERTMANAGER	EMAIL	VARCHAR2	100	112		7	100
5	HRMDB	EXPERTMANAGER	SOCIALNO	VARCHAR2	50	64		58	275

② Object 검색

DBMS 내부의 View, Trigger, Function, Procedure 등의 Object를 검색하여 암호화 대상 컬럼과 테이블을 포함하는 즉, DB 암호화에 영향을 받을 수 있는 Object를 추출한다.

예시) 추출된 Object

No	소유자 이름	테이블 이름	관련 트리거	관련 함수	관련 프로시져	관련 패키지
1	HRMDBA	ADMONIT			UPC_FINAL_REQUIRE	
2	HRMDBA	EDITLOG			UPC_FINAL_REQUIRE	
3	HRMDBA	EXPERTMANAGER		FN_CHECKREGIST	UPC_20110203	
4	HRMDBA	EXPERTMANAGERHISTORY			UPC_FINAL_REQUIRE	
5	HRMDBA	EXPERTMP			UPC_EXPERTREGFILETMP	

③ 쿼리 수집 및 분석

실제 DB에 접근하는 단위는 쿼리이며 전체 쿼리 요청 대비 암호화 쿼리 요청의 비율을 도출하여 암호화 이후 영향도를 분석할 수 있다. 전체 쿼리 요청량 수집, 암호화 쿼리 요청량 수집, 최적화 대상 쿼리 도출의 단계를 거친다.

- 전체 쿼리 요청량 수집 : 암호화 대상 DBMS에 요청되는 모든 쿼리에 대해 시간대별, 일별, 월별 등 전체 쿼리 요청량을 수집하여 DBMS의 피크 타임 추이를 분석
- 암호화 쿼리 요청량 수집 : 암호화 대상 DBMS에 요청되는 쿼리 중에서 암호화 대상 컬럼에 접근하는 쿼리에 대해 시간대별, 일별, 월별 등의 요청량을 수집하여 전체 쿼리 대비 암호화 쿼리의 비율을 분석
- 최적화 쿼리 도출 : 암호화 쿼리 중 최적화가 필요할 것으로 판단되는 유형의 쿼리를 분석

예시1) 수집된 쿼리에 대한 암호화 쿼리 / 최적화 쿼리 분석 결과

수집 쿼리수	암호화 쿼리수	최적화 쿼리수
5137	496	128

예시2) 일자별 전체 쿼리 요청량 / 암호화 쿼리 요청량

요청시간	전체 쿼리 요청량	암호화 쿼리 요청량
2011-03-06	47626	1597
2011-03-07	31651	1220
2011-03-08	24620	1260
2011-03-09	6603	1728
2011-03-10	51342	2944
2011-03-11	14261	1030
2011-03-12	2318	392
2011-03-13	6431	4732
2011-03-14	3821	933
2011-03-15	3230	1178

④ DBMS 분석

DBMS에 대한 리소스(예 : CPU, Memory, Storage 등)에 대해 확인하고 암호화 적용에 따라 적정 수준의 리소스를 확보해야 한다. 시스템 환경에 따라 차이가 있기 때문에 사전에 DB 운영 Health Check를 분석하여 기준 값을 설정하고 암호화 이후 변동될 수 있는 사항을 확인한다.

[표 16] DBMS 분석 시 고려사항

구분	주요 내용
CPU	현재 CPU 평균 사용량 및 변동 추이를 파악하여 암호화를 적용한 이후에 증가할 수 있는 부하에 대한 분석
Memory	현재의 메모리 사용량을 파악하고 암호화 적용에 따른 메모리 추가 소요에 대한 분석
Storage	도입 기술에 따라 기존 데이터에 대한 초기 암호화 적용을 위해 스토리지 공간을 많이 사용할 수 있으며 이에 대한 사전 분석 필요. 또한, 암호화 컬럼의 인덱스 수 및 테이블에 저장 시 Data Type에 따라 저장공간이 증가함으로 이에 대비한 여유공간 확보 필요.
DBMS 환경 설정	도입 기술에 따라 필요할 수 있는 DBMS 환경 설정 권고치를 미리 수집하여 기존 환경과의 적합성 파악

⑤ 응용 프로그램 분석

응용 프로그램의 모든 암호화 관련 쿼리를 수집하여 테스트하고 성능 최적화 방안을 수립한다. 사전에 성능 영향도를 분석함으로써 안전하게 암호화를 구축할 수 있다.

응용 프로그램 분석 단계는 아래와 같은 수행 단계를 거치게 된다.

- 암호화 관련 모든 쿼리를 수집
- 해당 쿼리에 대해 암호화 전 성능 및 암호화 후 성능 측정
- 암호화 후 성능이 느린 쿼리에 대해 최적화 작업 수행

예시) 쿼리 테스트 결과

쿼리 테스트 결과

업무	Table Name	쿼리	건수	암호화전	암호화후	결과	최적화후	최적화쿼리	최적화내용	소스반영	최종결과
RBP0003E	NEWWORK_MSTCHANGE\	SELECT *	1	0:00:00	0:00:00	정상					
RBP0003E	NEWWORK_MSTCHANGE\	SELECT	1	0:00:00	0:00:00	정상					
TCL0001E	CHANGEWORK_MST	SELECT	1	0:00:00	0:00:00	정상					
TCL0001E	CHANGEWORK_MST	SELECT	1	0:00:00	0:00:00	정상					
TCL0001E	CHANGEWORK_MST	SELECT	5	0:00:00	0:00:00	정상					
TCL0002E	CHANGEWORK_MST	SELECT	1	0:00:00	0:00:00	정상					
TCL0002E	CHANGEWORK_MST	SELECT	2	0:00:00	0:00:00	정상					
COL0004E	AU_USER_INFO	SELECT	1	0:00:00	0:00:00	정상					
COL0004E	AU_USER_INFO	SELECT	1	0:00:00	0:00:00	정상					
ATL0001E	AU_USER_INFO	SELECT	9	0:00:00	0:00:00	정상					
MultiAODFeedServiceDlg.(	NEWWORK_MST	UPDATE	0	0:00:00	0:00:00	정상					
MultiAODFeedServiceDlg.(	NEWWORK_MST	UPDATE	0	0:00:00	0:00:00	정상					
MultiAODFeedServiceDlg.(	NEWWORK_MST	UPDATE	5	0:00:00	0:00:00	정상					
MultiAODFeedServiceDlg.(	CHANGEWORK_MST	UPDATE		0:00:00	0:00:00	정상					
MultiAODFeedServiceDlg.(	NEWWORK_MST	SELECT TOP	20	0:00:02	0:00:09	최적화대상	0:00:02	SELECT TOP	복호화최소	0	정상
MultiAODFeedServiceDlg.(	NEWWORK_MST	SELECT TOP	0	0:00:00	0:00:00	정상					
MultiAODFeedServiceDlg.(	CHANGEWORK_MST	UPDATE	0	0:00:00	0:00:00	정상					

다. 테스트 검증

운영 환경과 동일한 테스트 환경을 구축하여 암호화를 적용한 후에 어플리케이션 등의 업무 테스트를 진행하는 단계이다. 테스트를 통해 운영 환경에 이행 시 발생할 수 있는 문제를 도출하고 모든 이슈를 해결하여 운영 환경에 대한 이행을 준비해야 한다.

해당 절차에서 컬럼암호화 방식의 경우, 사전 SQL검증 작업을 위해 Test DB(개발 DB)에서 먼저 암호화한 후 암호화된 테이블을 접근하는 모든 SQL들을 Test 및 검증해야 한다. 이 절차가 완료되면 운영 DB의 암호화 일정을 정하고, 상세한 Task별 실행 시나리오를 만든 다음 각각의 Task 별로 소요되는 시간을 측정하며 업무 프로세스를 감안하여 각각의 암호화 대상 테이블별로 암호화 순서를 정한다. 블록 암호화 방식은 SQL 검증 작업에 비중을 두지 않고 주요 업무에 대한 테스트 검증을 수행한다.

일반적으로 Test DB 서버와 운영 DB 서버의 사양이 다르기 때문에 정확한 소요 시간을 측정하기 위해서는 Test DB에서 암호화 한 테이블을 운영 DB에서도 암호화 해 보면 H/W의 성능 차이에 의한 암호화 시간 차이를 알 수 있다. 이를 근거로 소요 시간을 산정하면 된다.

먼저 테스트 환경은 운영 환경과 동일한 데이터와 어플리케이션을 준비한 후 암호화 대상 테이블/컬럼을 암호화하여 성능 및 이상 처리 여부를 확인한다. 만일 문제가 발견되면 SQL 수정을 통해 해결토록 하고 수정된 SQL이 반영된 어플리케이션을 따로 준비해 둔 후, 운영 시스템의 암호화가 종료되면 수정된 어플리케이션으로 교체하는 순서로 진행한다.

※ Plug-In 방식의 경우, 암호화 적용 이후에 발생할 수 있는 성능 저하를 최소화하기 위해 쿼리 최적화 작업을 수행

운영 중인 업무와 관련된 DB 암호화에서는 이미 사용되고 있는 어플리케이션 내의 SQL문들의 Test가 가장 중요하며 많은 시간이 소요된다. 이 부분의 Test/검증 정확도에 따라 프로젝트의 성공 여부가 결정지어 진다. 따라서 어플리케이션 개발/운영 조직의 협조가 매우 중요하다.

운영 중인 업무와 관련된 DB 암호화와는 달리 차세대 등의 어플리케이션 재개발 시에 적용하게 되면 SQL문의 테스트 과정이 생략될 수 있고 최적의 성능이 실현될 수 있는 등 다양한 방법 적용이 가능하다.

(그림 14) 테스트 검증 절차 비교

라. 구축 및 안정화

테스트 단계에서 검증된 사항을 종합하여 운영 환경에 DB 암호화를 적용하는 단계이다. 데이터에 대한 암호화 적용뿐만 아니라 테스트 검증 단계에서 변경된 소스코드 또는 최적화 쿼리를 함께 반영해야 한다. 또한, 테스트를 통해 도출된 이슈를 해결하여 운영환경에 적용하여야 한다.

실제 운영 시 시스템의 안정화를 위해서는 DB 보안관리자 및 DB관리자와 어플리케이션 개발자에 대한 교육을 실시하여 DB 암호화 솔루션의 안정적인 운영 및 관리를 위한 기술이 전수되도록 하고, 지속적인 모니터링을 수행해야 한다.

제6장 맺음말

본 가이드는 국내에 알려진 DB 암호화 기술을 살펴보고, DB 암호화 도입 시 고려사항 및 구축방안을 제시하였다. 본 가이드에서 제시된 고려사항은 다음과 같다.

- 암호화 대상
  : 적용 여부 및 적용범위를 결정하고 국내 법·규정에 명시된 정보(비밀번호 또는 바이오정보, 주민등록번호 등)를 우선으로 암호화 대상 선정

- 암호화 알고리즘
  : 보안강도 및 안전성을 고려하여 암호알고리즘 선정, 안전성이 검증된 암호 모듈 및 안전한 운영모드를 적용

- 암·복호화 범위
  : 각 기술의 암·복호화 처리 시점, 데이터 특성 및 활용도 등을 고려하여 적합한 기술 적용

- 암·복호화 키 관리
  : 암복호화 키 및 마스터 키의 생성·분배·저장·사용·백업/복구·교체·폐기 시 안전하게 관리

- 암·복호화
  : 암·복호화 시 인덱스 검색 설정, 부분암호화 적용, 데이터 저장 공간 확보, 원본데이터 삭제, 성능 부하 등을 고려하여 암·복호화 수행

- 접근통제
  : 암호화 데이터, 암·복호화 키 등의 보안성 유지를 위한 접근통제 (권한 분리. 사용자 인증 및 식별) 구현

- 암호통신
  : 송·수신 데이터 보호를 위한 암호 통신 구현

- 보안감사
  : 정책 및 암·복호화키 변경, 접근 내역, 성능 변화 등 기록 및 관리

개인정보의 보호가 중요한 보안 화두로 제기되는 시점에서 보안 담당자는 조직의 중요 정보를 보호하기 위해 DB 암호화 요구사항 및 운영 환경에 적합하게 기술을 도입하는 것도 중요하나, 구성 이후에도 주기적으로 운영·관리하면서 안정성과 효율성을 높여가는 것이 더욱 중요함을 인식해야 한다.

향후에는 기업이 보유하게 되는 고객 정보의 양이 점점 방대해지고 빅데이터 활용 등 데이터의 가치는 높아질 것으로 예상되므로 이에 대비한 보안 대책도 간과하여서는 안 될 것이다.

[붙임 1] 사전 협의 시 고려사항

구분	내용
암·복호화	암호화 적용 데이터 선정 (데이터 특성, 활용도 등 고려)
	암호화 데이터 타입(Integer, Character, String 등)
	지원 암호화 알고리즘
	안전한 암호 모듈 및 난수 발생기 이용 여부
	테이블(파티션 테이블, 클러스터 포함), 인덱스, 컬럼 단위 등으로 선택적 암호화 지원
	Primary Key 암복호화 지원
	Trigger 및 Default값의 암호화 지원
	NULL 데이터 암호화 지원
	암호화 적용 후 인덱스 검색 지원
구축	유추해석이 불가능한 운영모드 지원
	특정 데이터 타입 컬럼으로 인해 다른 컬럼의 암호화 제약 여부
	암호화 결과 저장 데이터 타입
	원본데이터 복구 가능 여부(초기 암호화 중 문제 발생 시 필요)
	안전한 암복호화 키 생성 및 관리 여부
	암복호화 키, 핵심보안 매개변수 등 평문 저장 금지 여부
	암호 모듈 종료 시 암·복호화 키 및 핵심보안 매개변수 제로화 여부
	암호화 완료 후 DB 내부에 저장된 원본데이터 제거 여부
	현재 사용 중인 소프트웨어와의 호환성 지원
	초기 암호화 구축이나 추가 암호화 작업 시 무중단 암호화 지원 (과도한 Lock 발생 여부)
	기존 어플리케이션의 수정 필요성 여부
	암호화 후 기존 테이블의 Dependency, Constraint 불변
	암호화 시 테이블 및 인덱스의 다른 테이블 스페이스 이동 지원

구분	내용
성능	암호화 데이터 입력 및 조회 시 시스템 자원 사용률의 적정성(CPU 사용률, 메모리 사용량)
	암호화 데이터 입력 및 조회 시, 단위 시간당 데이터 트랜잭션 수
	암복호화 서버 부하 분산 방안
운영	다양한 운영체제 지원 여부
	다양한 DBMS 지원 여부
	OS 및 DBMS의 업그레이드에 독립적
	암·복호화 키 장비 또는 암호화 수행 서버의 이중화 구성 가능 여부
	네트워크 또는 암호화 제품 장애로 인한 구축중단 또는 서비스 중단 가능성 및 대응 가능 여부
	암호화된 컬럼에 대한 배치 시 일반 DML 처리 여부
보안	암복호화 권한 및 접근통제 지원
	데이터 접근 및 작업, 암·복호화 처리, 정책 설정, 암·복호화 키의 변경, 성능 변화 등 다양한 로그 기록
	암호화 데이터, 정책 및 암복호화 키 등 백업, 복구 수행
	로그 백업 및 위변조 방지 지원 여부
	시스템 간 암호화 통신 지원 여부

[붙임 2] 관련 법률 및 규정

1. 개인정보보호법

개인정보보호법 상의 개인정보란 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보' (해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)로 고유식별정보(개인정보)를 처리하는 경우에 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 등 안전성 확보에 필요한 조치를 하도록 규정하고 있다.

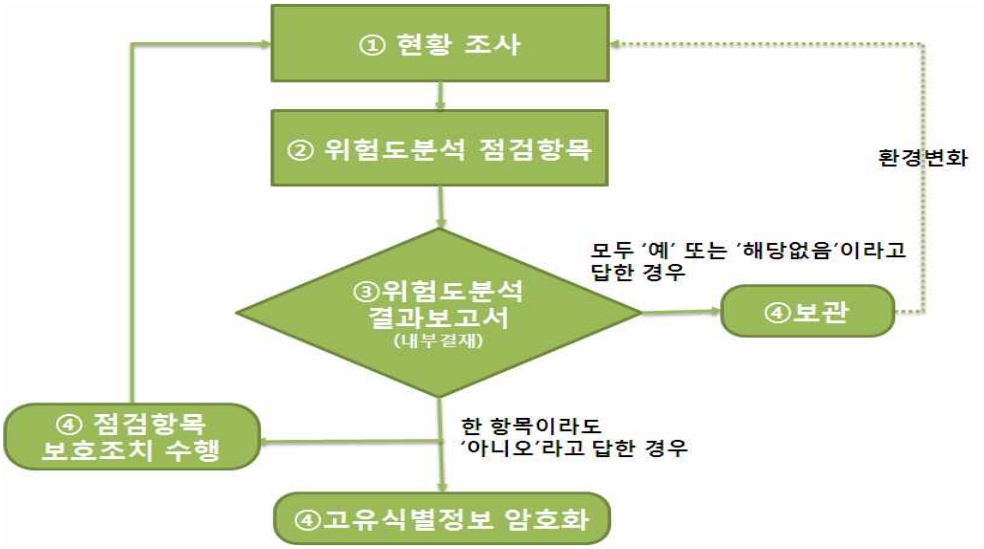
2016년 1월 1일에 시행될 제24조의2(주민등록번호 처리의 제한) 조항은 주민등록번호는 원천적으로 처리할 수 없도록 규정하고, 금융회사 등 주민등록번호 처리가 불가피한 경우 주민등록번호는 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 조치를 수행하여 안전하게 보관하도록 하였다. 그러므로, 다른 고유식별 정보에는 암호화 조치와 준하는 방법으로 안전성 확보 조치를 수행하였음에도 불구하고, 주민등록번호는 반드시 암호화 조치를 취하여 보호하여야 한다.

가. 위험도 분석 기준

위험도 분석 기준 결과에 따라 암호화 적용여부 및 적용범위를 정하여 DB 암호화를 시행할 수 있다. 개인정보처리자는 암호화 기술 적용 또는 이에 상응하는 조치를 완료해야 한다.

위험도 분석은 개인정보처리시스템에 적용하고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 침해할 위험의 정보를 위험도 분석기준을 이용하여 분석하는 것이다. 최초 분석 후에도 개인정보처리시스템을 증설 등 운영환경이 변경되는 경우 지속적으로 실시하여야 한다. 위험도 분석 기준은 내부망에 고유식별정보를 암호화하지 않고 저장하는 경우 개인정보처리자가 이행해야하는 최소한의 보호조치 기준으로 ①현황 조사, ②위험도 분석 점검 항목, ③위험도 분석 결과 보고서로 구성되어 있으며 절차는 (그림 16)와 같다.

(그림 15) 위험도 분석 기준 구성



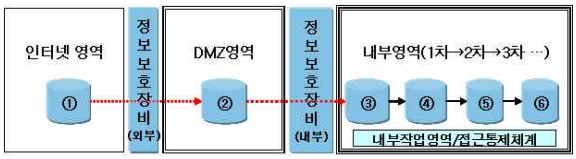
(그림 16) 위험도 분석 절차

위험도 분석을 위해 먼저 개인정보처리시스템을 기준으로 해당 시스템이 보유하고 있는 개인정보파일[25]의 취급 개인정보, 네트워크 연결여부, 보유량, 개인정보처리시스템명 등을 파악하고 아래 [표 17]을 참고하여 고유식별정보 보유 현황을 조사한다.

[표 17] 고유식별정보 보유 현황

점 검 항 목	비 고
1. 취급하는 고유식별정보에 해당되는 항목을 모두 체크하여 주십시오. ① 주민등록번호 ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호	o ①~④번 항목에 해당사항이 없을 경우 고유식별정보 암호화 의무 대상이 아닙니다.

25) 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)

점 검 항 목	비 고
2. 1번 항목에서 취급하는 개인정보를 어떻게 저장하고 있습니까? ① 모든 항목 암호화 저장 ② 일부 항목 암호화 저장 ③ 암호화 하지 않고 저장	o ①번 항목 선택 시에는 이미 암호화 중이므로 위험도 분석을 할 필요가 없습니다.
3. 개인정보파일의 저장위치는 어디 입니까? ① 인터넷 영역 ② DMZ영역 ③ 내부영역(업무망) ※ 아래 그림을 참고하여 해당 개인정보의 저장·검색·편집·정정 등을 위한 개인정보처리시스템(DB 등)이 위치하고 있는 번호에 체크하십시오.  	o ①번 또는 ②번 항목 선택 시 위험도 분석 점검표와 관계없이 암호화 대상입니다.

조사된 개인정보파일 단위별로 위험도 분석 항목에 따른 점검을 수행한다. 점검항목은 아래 [표 18] 과 [표 19]를 참고한다.

[표 18] (기관 기준) 점검 항목

구 분	점 검 항 목
정책기반	1. 개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?
	2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?
	3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?

	4. DB 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립·운영하고 있습니까?
	5. DB 서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시하고 있습니까?
네트워크 기반	6. 상시적으로 비인가 IP주소의 접근을 통제하고 있습니까?
	7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?
	8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?
	9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?
	10. 주기적으로 네트워크 접속에 대한 로그를 관리하고, 분석하고 있습니까?
	11. 네트워크 장비 및 정보보호시스템의 보안패치 발생 시 지체없이 업데이트를 수행하고 있습니까?

[표 19] (개인정보처리시스템 기준) 점검 항목

구 분	점 검 항 목
DB 및 어플리케이션 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?
	13. DB 서버 내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?
	16. DB 서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?

구 분	점 검 항 목
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동 발생시 지체없이 DB 접근권한을 변경하고 있습니까?
	19. DB 접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?
	20. DB 접속자 및 개인정보취급자의 비밀번호 입력시 5회 이상 연속 입력 오류가 발생한 경우 계정잠금 등 접근을 제한하고 있습니까?
	21. DB 및 DB 접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?
	22. DB 및 DB 접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?
	23. DB 서버 및 DB 접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?
	24. HDD등 DB 저장매체의 불용처리 시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
웹(Web) 기반 ※ 웹사이트를 운영하는 경우에만 해당	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?

위험도 분석 기준의 증적과 위험도 분석 점검에 따른 암호화 여부 등 위험도 분석 결과를 작성한다. 다음 (그림 17)은 결과보고서의 예시이다.

(그림 17) 위험도 분석 결과보고서

위험도 분석 결과보고서

작성일	년 월 일	작성자	(소속) (성명)
개인정보파일명			

(작성예제)

< 목 차 >

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)에서 규정하는 개인정보의 보호조치로 기술적·관리적 조치를 하여야 하며, 그 조치 기준의 하나로 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안조치를 하도록 한다.

최근 개인정보의 암호화 의무를 현실에 맞게 개선하기 위해 일부 법률 개정의 움직임이 있으며, 개정되는 법률 및 시행령에는 지문, 홍채 인식 등 바이오정보를 기존 '일방향 암호화' 대신 '양방향 암호화' 기술을 적용하도록 하여 실질적 활용이 가능토록 하고, 암호화 대상의 추가·변경이 용이하도록 암호화 대상을 고시로 명시할 예정이다. 향후 정보통신망법 개정에 따라 법률에서 규정하는 암호화 대상 범위 및 방식이 변동될 가능성이 있다.

3. 감독규정

금융회사에서 준수하여야 하는 전자금융감독규정과 신용정보업감독규정에서 데이터 암호화를 적용하도록 규정하고 있으며, 각 규정에 명시된 내용은 다음과 같다.

[표 20] DB 암호화 관련 감독규정 내용

구분	내용
전자금융감독규정	DMZ구간 내에 거래로그를 관리하기 위한 경우 암호화하여 저장·관리하고 내부사용자 및 이용자 비밀번호 암호화하여 보관
신용정보업감독규정	신용정보회사에 대해 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해 일방향 암호화하여 저장

[첨부]

1. 개인정보 보호법 · 시행령

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
	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.**	
제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게	제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.	제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우 ② 삭제 <2013.8.6.> ③ **개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는**	1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 **2. 개인정보에 대한 접근 통제 및 접근권한의 제한 조치** **3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치** 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 5. 개인정보에 대한 보안프로그램의 설치 및 갱신 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등	최소한의 범위로 **업무 담당자에 따라 차등부여**하여야 한다. ② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 **개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소**하여야 한다. ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다. ④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, **개인정보취급자 별로 한 개의 사용자**

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다. ④ 삭제 <2013.8.6.> 제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 3. 제1호 및 제2호에 준하여 주민등록번호	물리적 조치 ② 안전행정부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 안전행정부장관이 정하여 고시한다	**계정을 발급**하여야 하며, 다른 개인정보 취급자와 공유되지 않도록 하여야 한다. 제6조(접근통제 시스템 설치 및 운영) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다. **1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한** **2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지**

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
처리가 불가피한 경우로서 안전행정부령으로 정하는 경우 ② **개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·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.** ③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를		② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 **개인정보처리시스템에 접속 하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용**하여야 한다. ③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다. ④ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다. ④ 안전행정부장관은 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다. 제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.		만을 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다. 제7조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 **개인정보는 고유식별정보, 비밀번호 및 바이오정보**를 말한다. ② 개인정보처리자는 제1항에 따른 **개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화**하여야 한다.

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
		③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 **비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하**여야 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

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
		대상이 되는 **공공기관의 경우**에는 해당 **개인정보 영향평가의 결과** 2. **위험도 분석에 따른 결과** ⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 **안전한 암호알고리즘으로 암호화하여 저장**하여야 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 적용**하여야 한다. 단 **인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별**

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
		정보를 저장하는 경우 위험도 분석과 관계없이 암호화를 적용하여야 한다. 1. 개인정보의 저장 현황분석 2. 개인정보의 저장에 따른 위험도 분석 절차(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. 제8조(접속기록의 보관 및 위·변조방지) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소

개인정보 보호법 [시행 2014.3.24.] [법률 제12504호, 2014.3.24., 일부개정]	개인정보 보호법 시행령 [시행 2013.3.23.] [대통령령 제24425호, 2013.3.23., 타법개정]	개인정보의 안전성 확보조치 기준 고시 제정 2011.09.30. 행정안전부고시 제2011 - 제43호
		6개월 이상 보관·관리하여야 한다. ② 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

2. 정보통신망법 · 시행령

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2014.5.28.] [법률 제12681호, 2014.5.28., 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [시행 2014.1.1.] [대통령령 제25050호, 2013.12.30., 타법개정]	개인정보 기술적 · 관리적 보호조치 기준 개정 2012. 08. 23. 방송통신위원회 고시 제2012-50호
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. 1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행 **2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근**	제15조(개인정보의 보호조치) ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다. 1. 개인정보 관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항 2. 개인정보취급자의 교육에 관한 사항 3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한	제4조(접근통제) **① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.** **② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.** **③ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한**

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2014.5.28.] [법률 제12681호, 2014.5.28., 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [시행 2014.1.1.] [대통령령 제25050호, 2013.12.30., 타법개정]	개인정보 기술적 · 관리적 보호조치 기준 개정 2012. 08. 23. 방송통신위원회 고시 제2012-50호
통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 **4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치** 5. 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 ② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.	세부 사항 ② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다. **1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하**	**내역을 기록하고, 그 기록을 최소 5년간 보관한다.** ④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다. ⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다. **1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한** **2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보**

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2014.5.28.] [법률 제12681호, 2014.5.28., 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [시행 2014.1.1.] [대통령령 제25050호, 2013.12.30., 타법개정]	개인정보 기술적 · 관리적 보호조치 기준 개정 2012. 08. 23. 방송통신위원회 고시 제2012-50호
	"개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행 2. 개인정보처리시스템에 대한 침입차단 시스템 및 침입탐지시스템의 설치·운영 3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단 4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영 5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치 ③ 법 제28조제1항제3호에 따라 정보통신	유출 시도를 탐지 ⑥ 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다. ⑦ 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다. ⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다. 1. 다음 각 목의 문자 종류 중 2종류

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2014.5.28.] [법률 제12681호, 2014.5.28., 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [시행 2014.1.1.] [대통령령 제25050호, 2013.12.30., 타법개정]	개인정보 기술적·관리적 보호조치 기준 개정 2012. 08. 23. 방송통신위원회 고시 제2012-50호
	서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다. 1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독 2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 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**	이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 가. 영문 대문자(26개) 나. 영문 소문자(26개) 다. 숫자(10개) 라. 특수문자(32개) 2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 ⑨ 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2014.5.28.] [법률 제12681호, 2014.5.28., 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [시행 2014.1.1.] [대통령령 제25050호, 2013.12.30., 타법개정]	개인정보 기술적·관리적 보호조치 기준 개정 2012. 08. 23. 방송통신위원회 고시 제2012-50호
	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** ⑤ 법 제28조제1항제5호에 따라 정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로	공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다. 제6조(개인정보의 암호화) ① 정보통신서비스 제공자 등은 **비밀번호 및 바이오정보는 복호화되지 아니하도록 일방향 암호화**하여 저장한다. ② 정보통신서비스 제공자 등은 **주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화**하여 저장한다. ③ 정보통신서비스 제공자 등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2014.5.28.] [법률 제12681호, 2014.5.28., 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [시행 2014.1.1.] [대통령령 제25050호, 2013.12.30., 타법개정]	개인정보 기술적 · 관리적 보호조치 기준 개정 2012. 08. 23. 방송통신위원회 고시 제2012-50호
	갱신·점검하여야 한다. ⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다	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 제공자 등은 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

3. 전자금융감독규정

전자금융감독규정
[시행 2014.1.1.]
[금융위원회고시 제2013-44호, 2013.12.31., 타법개정]

제13조(전산자료 보호대책)

① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.

1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
4. **전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것**
5. 전산자료 및 전산장비의 반출·반입을 통제할 것
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것 <개정 2013.12.3>
7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것
9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 부하 테스트 등 사용이 불가피한 경우 이용자 정보를

변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)

11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것
13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)
14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.

③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.

④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.

1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

전자금융감독규정

[시행 2014.1.1.]

[금융위원회고시 제2013-44호, 2013.12.31., 타법개정]

⑤ **금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다.** 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다.

제17조(홈페이지 등 공개용 웹서버 관리대책)

① 금융회사 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 접근 제어 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 공인인증서등을 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 금융회사 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 삭제 <2013.12.3>

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 다음 각 호에 대하여 적절하게 대응 조치하여야 한다. <개정 2013.12.3>

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

전자금융감독규정

[시행 2014.1.1.]

[금융위원회고시 제2013-44호, 2013.12.31., 타법개정]

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

제32조(내부사용자 비밀번호 관리) 금융회사 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. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 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

전자금융감독규정

[시행 2014.1.1.]

[금융위원회고시 제2013-44호, 2013.12.31., 타법개정]

제33조(이용자 비밀번호 관리)

① **금융회사 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 금융회사 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. 금융회사가 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

4. 신용정보업감독규정

신용정보업감독규정
시행 2014.6.11.]
[금융위원회고시 제2014-13호, 2014.6.11., 일부개정]

제20조(기술적·물리적·관리적 보안대책) 영 제16조제1항에 따라 신용정보회사등이 마련해야 할 기술적·물리적·관리적 보안대책의 구체적인 기준은 별표 3과 같다.

[별표3] 기술적·물리적·관리적 보안대책 마련 기준(제20조 관련)

Ⅰ. 목 적

이 기준은 영 제16조제1항에서 정하는 신용정보의 기술적·물리적·관리적 보안대책과 관련된 구체적인 기준을 정함을 목적으로 한다.

Ⅱ. 기술적·물리적 보안대책(중략)

3. 개인신용정보의 암호화

① **신용정보회사등은 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해서는 복호되지 아니하도록 일방향 암호화하여 저장한다.**

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

신용정보업감독규정

시행 2014.6.11.]

[금융위원회고시 제2014-13호, 2014.6.11., 일부개정]

2. 웹서버에 암호화 응용프로그램을 설치하여 개인신용정보를 암호화하여 송수신하는 기능

③ 신용정보회사등은 개인신용정보를 PC에 저장할 때에는 이를 암호화해야 한다.(생략)

약 어

DBMS : DataBase Management System

DDL : Data Definition Language

ERD : Entity Relation Diagram

HSM : Hardware Security Module

RDBMS : Relational DataBase Management System

SQL : Structured Query Language

TDE : Transparent Data Encryption

WAS : Web Application Server

참고 문헌

[1] 암호 알고리즘 및 키 길이 이용 안내서, 한국인터넷진흥원, 2010.

[2] 개인정보 DB 암호화 관리 안내서, 한국인터넷진흥원, 2010.

[3] Best Practice for Database Encryption Solutions, Protegrity Corporation

[4] DB 암호제품 보안요구사항, IT보안인증사무국, 2010.

[5] 보다 안전한 정보화 자원 보호를 위한 DB 보안시스템 구축 방안에 관한 연구 : DB 암호화, 접근제어, 감사 시스템 통합, 이종열, 2005.

[6] 개인 프라이버시 보호 관점의 DB 암호화 도입 방법론, 김태균, 2010.

[7] SEED 암호 알고리즘을 이용한 데이터베이스 칼럼 단위 암호화에 관한 연구, 박정희, 2006.

[8] 금융부문 암호기술 관리 가이드, 금융보안연구원, 2009.

[9] Guide to protecting the Confidentiality of Personally Identifiable Information, NIST, 2009.

[10] http://www.dbguide.net

[11] 사업자의 개인정보 보호조치 기준, 행정안전부, 2010.

[12] 개인정보의 기술적·관리적 보호조치 기준, 방송통신위원회, 2011.

[13] 고객정보보호를 위한 DB 암호화 구현 사례, 삼성 SDS, 2003

[14] DB 암호화 솔루션 도입 시 고려사항 검토, 금융보안연구원, 2008.

[15] 개인정보의 기술적·관리적 보호조치 기준 해설서, 한국인터넷진흥원, 2009.

[16] 데이터베이스 암호화 기술과 제품 동향, ETRI, 2007

[17] The role of encryption in database security, Chirstian Kirsch, 2009

[18] 프라이버시를 보장하는 SQL 쿼리 가능한 데이터베이스, 박현아 외 2명, 2007

[19] 개인정보 위험도 분석 기준 및 해설서, 행정안전부·한국인터넷진흥원, 2012

[20] 개인정보 보호기술 동향 보고서, 금융보안연구원, 2011

[21] Data Breach Investigations report, Verizon, 2009 ~ 2012

[22] 데이베이스 보안 가이드라인, 한국데이터베이스진흥원, 2014

[23] DB 암호화 적용 시 성능향상 방법에 대한 모델 연구, 배계섭, 2011

[24] 암호 알고리즘 및 키 길이 이용 안내서, 한국인터넷진흥원, 2013

[25] 암호기술 구현 안내서, 한국인터넷진흥원, 2011

본 가이드 작성을 위해 다음 분들께서 수고하셨습니다.

2014년 12월

총괄책임자	금융보안연구원	본부장	조규민	
참여연구원	보안기술연구팀	팀장	임형진	
		연구원	김태희	
전자금융보안기술자문위원회				
위원장	충남대학교	교수	류재철	
위원	순천향대학교	교수	곽 진	
	강원대학교	교수	김상춘	
	한국과학기술원	교수	김용대	
	서울여자대학교	교수	김윤정	
	고려대학교	교수	김휘강	
	정보통신기술진흥센터	C P	원유재	
	숭실대학교	교수	정수환	
	한국인터넷진흥원	단장	정현철	
	국민대학교	교수	한동국	

외부전문가 : 마이크로소프트, 보메트릭, 세이프넷, 신시웨이, 오라클, 이글로벌, 이니텍, 컴트루테크놀로지

DB 암호화 기술 가이드

발 행	2014년 12월
발행인	김 영 린
발행처	금융보안연구원
주 소	서울특별시 영등포구 의사당대로 143 금융투자협회 빌딩 8, 9F