해외의 키관리서버 제품들과 우리나라의 해당 법규정 및 정책 설정의 필요성

김지현*

*고려대학교 정보보호대학원

Foreign Key Management Server Products and the necessity of Korean Related Law and Policy

Ji Hyun Kim*

*Graduate School of Information Security, Korea University

E-mail : mmlpl@hanmail.net

요 약

2012년 3월과 8월부터 개정된 개인정보보호법과 정보통신망법이 시행되면서 회사와 공공기관들은 법규가 요구하는 보안장비들을 갖추게 되었다. 암복호화 키가 유출되면 모든 정보를 공격자가 볼 수 있기 때문에 개인정보의 보호를 위해 키를 제3자가 알지 못하게 잘 보호,관리하는 것은 매우 중요하다고 볼 수 있다. 따라서 현재 보안업계에서는 키관리서버의 중요성이 점차로 대두되고 있다.키관리서버란 암복호화키를 안전하게 저장, 관리할 수 있는 어플라이언스 형태의 하드웨어 장비이다.본 논문에서는 해외의 키관리서버 제품들에 대해 알아보고 우리나라의 관련 법규정 입법 및 정책설정의 필요성에 관해 논의해 보겠다.

ABSTRACT

Personal Information Protection Law and Information Communication Network Law is administered from March, 2012 and August,2012.It is very important to protect and manage the key well so that the third party doesn't know the key. Thus, at present, there increases an importance of Key Management Server. Key Management Server is an appliance type of hardware equipment which can securely store and manage encryption and decryption key. In this paper, we will survey on foreign key management server products and discuss about the necessities of legislation of related law and establishment of policy.

키워드

안전조치의무, 키, 개인정보 보호, 키관리 서버

Ⅰ. 서 론

개인정보보호법이 2012년 3월 30일부터 시행되고 정보통신망법은 2012년 8월 18일부터 개정법이 시행되면서 회사나 공공기관들은 법규가 요구하는 보안장비들을 갖추게 되었다. 보안에 필요한 암호화, 복호화 과정에서는 송신자와 수신자가 알고 있는 키가 사용되는데 제3자는 송신자와 수신자의 키를 알지 못함으로 평문의 내용을 쉽게 알지 못할 것이다. 따라서 키가 외부로 유출되지 못하도록 보안하는 것은 '개인정보의 보호'에 있어서 중요하다고 볼 수 있다. 따라서 키를 제3자가 알지 못하게 강력하게 보호하는 수단이 필요하다. 본 논문은 2장에서 해외의 유명한 키관리서버 제품들의 특징과 기능에 관해 살펴보고 3장에서는 현행 법규의 안전조치의무에 관한 규정내용 그리고 마지막 4장에서는 우리나라의 관련 법규정 입법 및 정책 설정의 필요성에 관해 살펴보

1) 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정"지원사업의 연구결과로 수행되었음

겠다.

Ⅱ.해외의 키관리서버 제품들

(1)SafeNet의 DataSecure

세이프넷의 데이터 시큐어는 정보의 생성 접근, 저장, 공유 그리고 파기까지의 전 수명주기에 걸쳐 데이터를 중앙집중적으로 보호하는 암호화 전용 하드웨어 장비이다. 이 데이터 보호 솔루션은 토큰화 기술을 사용하는데 토큰화 기술이란 보호할 데이터를 토큰으로 치환하여 원본데이터 대신 토큰을 사용하는 기술이다. DataSecure에서는 모든 암호화 키가 중앙집중형 강화 어플라이언스에 저장된다.FIPS 140-2레벨2 인증, CC EAL-2인증을 받았다. FIPS(연방 정부 정보처리 표준) 140-2는 IT제품이 기밀은 아니지만 민감한 용도로 사용될 때 충족해야 할 암호화 및 관련 보안 요건을 규정한 미정부 표준이다. FIPS 140-2 표준은 승인되고 강력한 암호화 알고리즘 및 방식과 같은 안전한 보안수단이 제품에 사용되고 있음을 보증한다. 또한 개별 또는 다른 프로세스들이 제품을 활용하기 위하여 어떻게 승인되어야 하는지와 모듈이나 구성품이 다른 시스템과 안전하게 상호작용하기 위하여 어떻게 설계되어야 하는지를 규정한다. FIPS140-2에는 4가지 보안레벨이 정의되어 있는데 레벨2는 개별 사용자 인증은 필요하지 않고 역할 기반 인증이 필요하다. 또한 물리적 잠금장치 또는 부당 변경 검증수단을 사용하여 물리적 부당 변경을 감지할 수 있는 역량을 요구한다.[1]

(2)Thales의 Key Authority

Thales의 Key Authority는 다음과 같은 기능이 있다. 첫 번째, 시스템 백업과 복구기능이다. 탈레스의 Key Authority는 NFSv3(파일시스템 이름)을 사용해서 원격서버로 자동으로 백업을 받을 수 있다.두번째, 암복호화에 대한 리포팅 기능이 있다.셋째, 탈레스의 Key Authority는 IBM Storage와 테입솔루션과 연동해서 IBM스토리지 및 테입솔루션에 대해서 암호화, 암호화 가속 등의 기능을 하며 호환성을 제공한다. FIPS140-2 레벨3은 분해나 변용하기 어렵도록 물리적 부당 변경 방지 기술을 추가하여 해킹을 극도로 어렵게 만들어야 한다. 부당 변경이 감지되면 해당 장치는 중대한 보안변수를 삭제할 수 있어야 한다. 레벨3는 또한 강력한 암호화 보호와 키관리, ID 기반 인증 및 중대한 보안 변수가 입출력되는 인터페이스 간의 물리적/논리적 분리를 요구한다.

(3)Vormetric의 Core guard

Vormetric Core Guard는 미국 Vormetric사의 제품으로 Data암호화 및 상황 기반의 접근제어를 통해 중요 DB Data의 유출을 차단하는 통합 데이터 보안 솔루션이다.'상황 기반의 접근제어'란 누가, 무엇을, 언제, 어디서, 어떻게 라는 상황 기반의 데이터의 접근제어를 지원하는 것을 의미한다. 악성코드의 실행이나 허가받지 않은 어플리케이션의 구동을 막음으로써 시스템의 무결성을 보호한다. 3DES,AES128, AES256등 강력한 암호화 알고리즘을 제공한다. 다양한 이기종의 시스템 및 OS와 연동이 가능하다.

Ⅲ.안전조치의무

(1)개인정보의 안전성 확보 조치

개인정보보호법 제29조는 "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."라고 규정하고 있다.[5]개인정보보호법 시행령 제30조는 기존의 안전성 확보조치의 기준들을 유지하면서 법준수가 용이하도록 최소한의 기본조치 요구사항을 규정하고 있다.시행령 제30조 제1항은 안전성 확보조치에 관한 세부기준인 「개인정보의 안전성 확보 조치 기준」를 정하여 고시하고 있다.

(2)「개인정보의 안전성 확보 조치 기준」고시의 주요 내용

1)내부관리계획의 수립 및 시행(안전기준 제3조):

개인정보 처리자는 개인정보의 안전한 처리를 위하여 「안전기준」제3조 제1항 각호의 사항을 포함하는 내부관리계획을 수립, 시행하여야 한다(안전기준 제1항). 내부관리계획은 조직 내의 정보보호에 관한 헌법 또는 법률과 같은 역할을 수행하므로 전사적인 개인정보 보호 활동계획을 담아야 한다. 다음 각 호의 사항에 중요한 변경이 있는 경우에는 개인정보 처리자는 즉시 이를 반영하여 내부관리계획을 수정하여 시행하고 그 수정이력을 관리하여야 한다(안전기준 제3항). 다만, 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」제2조에 해당하는 소상공인은 내부관리계획을 수립하지 아니할 수 있다(안전기준 제2항).

【내부관리계획의 포함 내용(안전기준제3조제1항 】

1.개인정보 보호책임자의 지정에 관한 사항
2.개인정보 보호책임자 및 개인정보 취급자의 역할 및 책임에 관한 사항
3.개인정보의 안전성 확보에 필요한 조치 에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 그 밖에 개인정보보호를 위하여 필요한 사항

2)접근권한의 관리(안전기준 제4조)

(가)접근권한의 차등화: 개인정보 처리자는 개인정보처리시스템에 대한 접근권한을 업무담당자에 따라 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.

(나)접근권한의 변경, 말소: 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보 취급자가

변경되었을 경우에는 지체 없이 개인정보 처리 시스템의 접근권한을 변경 또는 말소하여야 한다.
(다)개별 사용자 계정의 발급: 개인정보 처리자는 개인정보 처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우 개인정보 취급자별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보 취급자와 공유되지 않도록 하여야 한다.
3)비밀번호 관리(안전기준 제5조): 개인정보 처리자는 개인정보 취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
4)접근통제 시스템 설치 및 운영(안전기준 제6조)
(가)접근통제 시스템 설치, 운영: 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각호의 기능을 포함한 접근통제 시스템을 설치, 운영하여야 한다.
【접근통제 시스템의 필수 기능】
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
다만, 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우에는 그러하지 아니할 수 있다. 이 경우에는 업무용 컴퓨터의 운영체제나 보안프로그램 등에서 제공하는 접근통제기능을 이용할 수 있다.
(나)안전한 원격 접속수단 강구:개인정보 처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN:Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다
(다)개인정보유출 방지 조치:개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.
5)개인정보의 암호화(안전기준 제7조):개인정보처리자가 정보통신망을 통하여 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호),비밀번호 및 바이오 정보(생체정보)를 처리하고자 하는 경우에는 암호화를 하여야 한다. 암호화는 해독이 어렵도록 안전한 암호알고리즘으로 하여야 하고, 특히 비밀번호를 처리할 때에는 복호화되지 않도록 일방향 암호화하여 저장하여야 한다. 정보통신 서비스 제공자의 경우에는 비밀번호 외에 바이오 정보, 주민등록번호, 신용카드번호, 계좌번호에 대해서까지 일방향 암호화를 하여야 하고, 신용회사정보 등도 역시 비밀번호 외에 바이오 정보(생체정보)에 대해서까지 일방향 암호화를 하여야 한다.
6)접속기록의 보관 및 위, 변조 방지(안전기준 제8조):개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관, 관리하여야 하며, 개인정보 취급자의 접속기록이 위, 변조 및 도난, 분시되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.
7)보안프로그램 설치 및 운영(안전기준 제9조): 개인정보처리자는 악성 프로그램 등을 방지, 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치, 운영하여야 하며, 보안프로그램의 자동 업데이트 기능을 사용하거나 1일 1회 이상 업데이트를 실시하여 보안 프로그램을 최신의 상태로 유지하여야 한다.
또한 악성프로그램과 관련한 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우에는 즉시 이에 따른 업데이트를 실시하여야 한다.
8)물리적 접근방지 조치(안전기준 제10조): 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우에는 이에 대한 출입통제절차를 수립 운영하여야 하고,개인정보가 포함된 서류, 보조저장매체 등은 잠금장치가 있는 안전한 장소에 보관하여야 하며, 휴대가 가능한 소형 스토리지 등은 고정장치로 고정하여야 한다.[2]

Ⅳ. 우리나라의 관련 법규정 입법 및 정책 설정의 필요성

중요 데이터를 보호하기 위한 정보보호의 핵심은 암호화 키의 보호와 관리이다.데이터 베이스가 암호화되어 있다 하더라도 암호화 키가 유출된다면 이를 통해 중요 데이터가 유출될 위험이 있다. 키관리 서버는 이러한 암호화 키를 안전하게 관리하고 보호할 수 있는 전용 하드웨어 시스템이다. 키관리 서버들은 일반적으로 다음과 같은 기능을 가지고 있다. 첫째, 키관리 기능이다. 키관리 기능이란 키를 보관하고 암복호화하는 것을 의미한다. 둘째, 백업 기능이다. 셋째, 로그(접속기록) 확인과 상태 확인 기능이다.[3] 우리나라에는 아직 키관리서버를 갖춰야 한다는 구체적인 법규정이 없어서 제품들도 거의 출시된 것들이 없지만 외국에는 이미 키관리서버의 일반적인 기능 이외의 다른 유용한 기능까지 갖춰서 출시된 제품들이 많다. 우리나라도 점점 공격의 유형이 다양해지고 보안에 대한 요구사항이 강화되면서 키를 잘 보호하기 위해 키관리서버의 도입필요성이 제기되고 있다. 키가 유출되면 다른 모든 보안장치가 무용지물이 된다. 이를 위한 관련 법규정이나 제도의 도입이 필요하다.

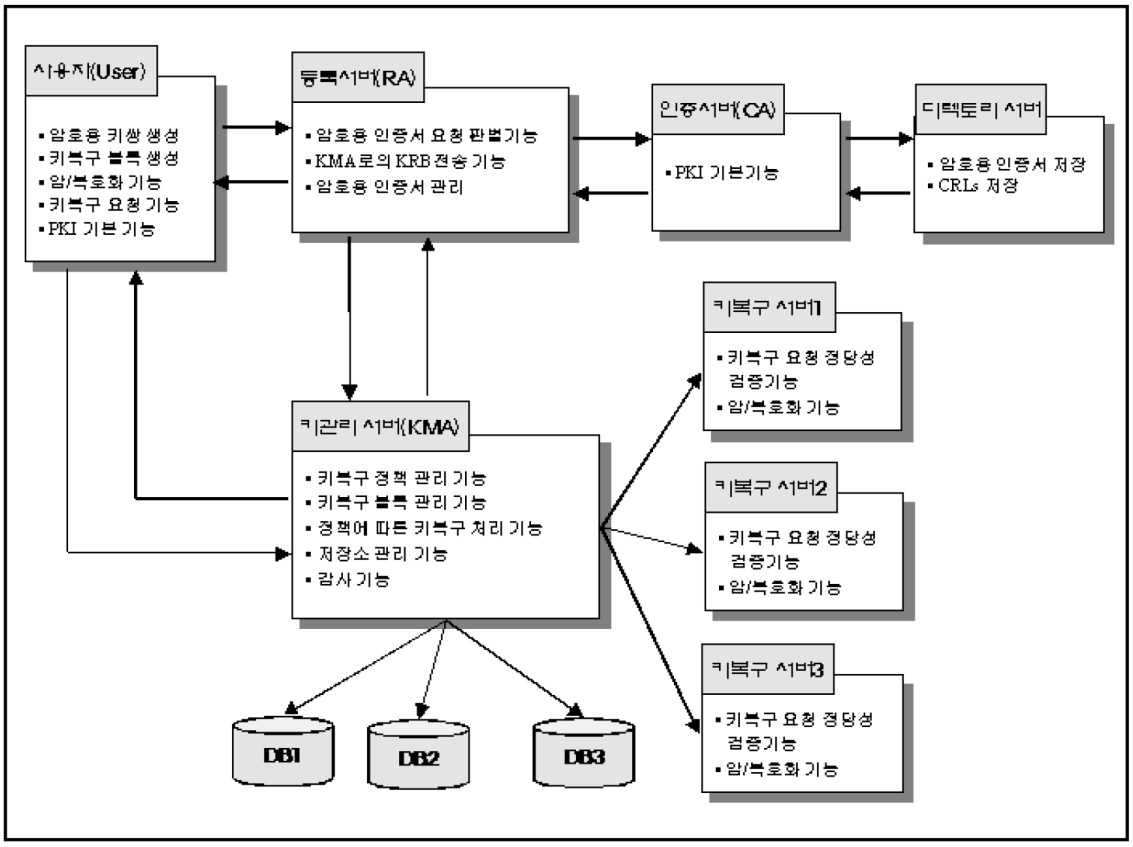

그림1. 한국정보보호진흥원의 상업용 암호키관리시스템

참고문헌

[1] Seagate, FIPS140-2표준 및 자체 암호화 드라이브 기술,마케팅 회보, 2010.07

[2] 이창범, 개인정보 보호법, 법문사,2012.01

[3] 권현조, 김지연, 박해룡, 암호용 키 및 인증서의 안전한 관리발급을 위한 암호키관리 기술, KISA,2005-08-09,

[4] 개인정보보호법