Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.2, Apr. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.2.397

개인정보 DB 암호화 검증 프레임웍 제안

고 영 대,[1,2†] 이 상 진[1‡]
[1]고려대학교, [2]법무법인 율촌

A Proposal of Personal Information DB Encryption Assurance Framework

Youngdai-dai Ko,[1,2†] Sang-jin Lee[1‡]
[1]Korea University, [2]Attorneys at Law Yulchon

요 약

지난 2011년 3월, 개인정보보호법 제정에 따라 업무적으로 암호화 대상이 되는 개인정보를 취급하는 개인정보처리자는 해당 개인정보처리시스템에 대한 DB 암호화를 적용해야 한다. 또한 이에 맞추어 법 집행 및 이행 기관인 관련 당국에서는 이러한 DB 암호화 규정이 제대로 적용되고 이행되고 있는지 관리 감독을 강화하고 있다. 그러나, DB 암호화라는 과정 자체가 시스템 및 업무 절차 등 현실적으로 고려해야 할 요소가 많고 DB 암호화 시 투입되는 시간 및 비용 또한 만만치 않다. 게다가 암호화 규정에 따른 암호화 기준 및 가이드에 비해 실질적으로 고려해야 할 요소들이 상당히 많음에도 불구하고 아직까지 암호화와 관련된 보다 구체적이고 현실적인 검증 항목이 다소 부족한 것으로 보인다. 이에 본 논문에서는 법규 준수의 의무가 있는 수범자, 즉, 개인정보처리자의 입장과 이러한 법규 준수에 대한 점검 및 통제 의무가 있는 관련 당국의 규제 기관 등에서 상호간 건전하고 합리적인 시각에서 DB 암호화에 대하여 현실적이고 구체적인 방향성을 제시하고자 DB 암호화 시 반드시 고려해야 할 DB 암호화 검증 프레임웍을 제안하고자 한다.

ABSTRACT

According to the Personal Information Protection Act(PIPA) which is legislated in March 2011, the individual or company that handles personal information, called Personal information processor, should encrypt some kinds of personal information kept in his Database. For convenience sake we call it DB Encryption in this paper. Law enforcement and the implementation agency accordingly are being strengthen the supervision that the status of DB Encryption is being properly applied and implemented as the PIPA. However, the process of DB Encryption is very complicate and difficult as well as there are many factors to consider in reality. For example, there are so many considerations and requirements in the process of DB Encryption like pre-analysis and design, real application and test, etc.. And also there are surely points to be considered in related system components, business process and time and costs. Like this, although there are plenty of factors significantly associated with DB Encryption, yet more concrete and realistic validation entry seems somewhat lacking. In this paper, we propose a realistic DB Encryption Assurance Framework that it is acceptable and resonable in the performance of the PIPA duty (the aspect of the individual or company) and standard direction of inspection and verification of DB Encryption (the aspect of law enforcement)
Keywords: Personal Information Protection Act, DB Encryption, Verification, Assurance, Framework

I. 서 론

2011년 3월에 제정된 개인정보보호법[9]에 따라 업무적으로 고유식별정보에 해당하는 개인정보를 취급하는 개인정보처리자는 해당 고유식별정보에 대하

접수일(2013년 11월 1일), 수정일(2014년 4월 1일), 게재확정일(2014년 4월 2일)
† 주저자, ydko@korea.ac.kr, ydko@yulchon.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

여 지난 2012년 12월까지 암호화 하도록 의무화 되었다. 개인정보보호법에서 말하는 고유식별정보란 주민번호, 외국인등록번호, 여권번호 및 운전자 등록 번호를 가리키며 고유하게 개인을 식별할 수 있는 정보를 뜻한다.

물론, 개인정보보호법 이전에도 정보통신망 이용촉진 및 정보보호에 관한 법률(이하 정통망법)[8]에 따른 정보통신서비스 제공자 등은 개인정보를 네트워크를 통해 전송하거나 DB에 보관할 경우 특정 개인정보에 대해서는 암호화하도록 하고 있었으나 이는 정보통신망을 통해 서비스를 제공하는 일부 기업에만 해당되었다. 이로 인해, 업무적으로 개인정보를 처리하는 경우에는 관련 법규에 의거 암호화 조치를 하거나 암호화에 상응하는 보호조치[6]에 따라 개인정보를 안전하게 보호하여야만 한다. 즉, 법적 강제화에 의거 개인정보를 통해 업무를 진행하고 해당 고객에게 서비스를 제공하는 입장에서 개인정보에 대한 암호화 조치는 필수 불가결한 법적 제재 수단이 되었다. 최근의 법 개정 동향에 따르면 이러한 암호화 대상 개인정보(특히, 주민번호) 부주의로 인한 유출사고 발생 시 그 책임의 수위 또한 높아지고 있어 관련 개인정보처리자 및 개인정보보호 업무를 담당하고 있는 실무자들의 기술적,관리적 보호조치 뿐만 아니라 주의 노력과 관심 또한 상당히 높아지고 있다. 일반적인 개인정보 보호를 위한 보호조치를 본 논문에서 다루는 것은 본 논문의 의도와는 다소 거리가 있어, 개인정보의 기술적 보호조치 중 가장 큰 핵심사안 중 하나라고 여겨지는 개인정보의 암호화, 특히 암호화 중에서도 DB암호화에 대하여 언급하고자 한다.

앞서 언급한 바와 같이 개인정보를 업무적으로 처리하는 대부분의 기업 및 기관에서 개인정보에 대한 암호화 조치를 하려는 주된 이유는 관련 법규를 준수하여, 법적 책임 요건을 준수하기 위함이다. 물론, 이를 통해 고객의 개인정보 보호 수준을 향상시킬 수 있는 효과는 얻을 수 있으나, 솔직히 말하자면 이는 부수적인 사안으로 자발적인 개인정보보호를 위한 조치가 아닌 타의적이고 수동적인 방어조치로 볼 수 있을 것이다.

그러나, 개인정보 보호에 관련된 안전행정부, 미래창조과학부, 방송통신위원회 및 이하 관계 당국의 입장은 아마도 다소 상이한 것으로 보인다. 암호화 대상 중 가장 문제가 되고 있는 주민번호 이용과 관련된 법규정 등을 신설하는 한편, 이러한 주민번호가 유출되었을 경우의 처벌 기준 또한 지속적으로 강화하고 있다. 개인정보보호법과 전자금융거래법 시행령에 대한 개정 내용을 통해서도 관계당국의 이러한 적극적인 규제 움직임을 엿볼 수 있다.

즉 수범자 입장에서는 최소한의 시간과 노력을 투자하면서 암호화 규정 준수를 위해 노력하려고 할 것이며, 관계 당국 입장에서는 해당 암호화 규제 조항의 법적 취지를 최대한으로 살리고자 할 것은 자명해 보인다. 그러나, 여기서 반드시 짚고 넘어가야 할 사항은 바로 암호화로 인한 시간적, 물질적 투자비용과 적용 시 발생가능한 기술적 이슈사항 및 암호화로 인한 업무 프로세스의 변경 등 다방면에 걸쳐서 고려해야할 부분들이 너무도 다양하다는 점이다. 조직 규모에 따라 다소 상이한 부분이 있겠으나, DB 암호화의 경우 적용 시 기업 환경 또는 시스템 구조에 따라 막대한 비용이 발생할 수 있다. 암호화 적용 시를 대비한 사전 영향평가 수행, 기존 어플리케이션 및 기반 인프라의 변경, 암호화 장애 시 비상 대응절차 마련 등 다방면에 걸친 준비 작업이 필요하기 때문이다.

이처럼 수범자 입장에서는 DB 암호화 적용을 위해 상당량의 인원, 비용과 시간 등의 막대한 내부 자원을 투자하여 암호화 조치를 완료하고도 일부 예상하지 못한 부분에 대한 암호화 관련 검증해야 할 일부 항목에 대한 소홀로 인해 관계 당국으로부터 과태료 또는 벌금 등의 행정처분을 당할 수도 있기에 이러한 위험 요소를 사전에 예방하기 위한 구체적인 기준이 필요한 실정이다. 또한, 관계 당국의 입장에서도 DB 암호화를 위한 구체적이고 실질적인 가이드 뿐만 아니라, 암호화 이후 또는 암호화 준비 시 반드시 고려해야할 기준, 즉, 수범자들이 DB 암호화를 적용함에 있어서 또는 적용 이후 운영 측면까지 고려한 구체적인 방향점을 제시할 필요가 있다고 할 것이다.

본 논문에서는 이렇듯 다양한 측면을 고려해야하는 DB 암호화라는 기술적 법규 이행사항에 대하여, 해당 조치를 준수해야 하는 수범자 입장의 관련기업 및 기관 등의 개인정보처리자와 더불어 해당 암호화 조치가 법적, 기술적 그리고 관리적으로 올바르고 최대한 안전하게 적용되었는지를 관리해야 하는 관련 당국의 입장에서 향후 DB 암호화 시 반드시 점검하고 고려해야 할 검증항목들에 대하여 살펴보고자 한다.

II. 선행 연구

지금까지의 DB 암호화와 관련한 관계당국의 주요 가이드 및 안내 지침 등에서 제시하고 있는 주요 내용

에 대해서 간략하게 살펴보고자 한다.

• KISA, 암호이용 안내서[1]

해당 안내서에서는 기업 및 기관의 시스템 관리자 및 보안관리자에게 자사가보유한 정보의 보안등급 및 이용단계에 따른 암호기술의 적용 수준과 범위, 교육, 의료 등 분야별 암호기술 활용방안을 제시하였다. 주로 기업의 중요 자료 보호를 위해 적용하는 암호화의 기술적 측면에 대한 적용 사례 및 방안에 대한 논의가 주가 되고 있다.

• KISA, 암호 알고리즘 및 키 길이 이용 안내서[2]

해당 안내서에서는 암호화에 있어서 핵심 역할을 담당하는 암호 알고리즘 및 키 길이와 해쉬함수에 대한 안전성 유지기간과 보안강도의 분석을 토대로 향후 기업에서 사용할 수 있는 암호 알고리즘에 대한 선택 기준 및 안전성을 가이드하고 있다.

• KISA, 개인정보 DB 암호화 관리 안내서[3]

해당 안내서에서는 개인정보보호를 위한 암호화 규정을 중심으로 국내·외 관련 법제도 재개정 현황을 토대로 해당 법률을 준수하기 위한 개인정보보호대책의 하나로 개인정보 DB 암호화 관리방안을 소개하고 있다. 주로 법률적인 법 조항 및 처벌 사항에 대한 규정들에 대한 사례를 가이드하고 있다.

• KISA, 기업 및 기관의 IT정보자산 보호를 위한 암호정책 수립 기준 안내서[4]

해당 안내서에서는 기업 및 기관이 암호정책 수립 시 참고가 될 수 있도록 국내 정보보호 관리체계 인증 제도 및 국제 표준에서 명시하는 요구사항에 적합한 암호정책 수립 기준을 제시하였다. 다만, 해당 설명서는 암호화 정책 수립에 있어서 필요한 대표적인 요건 즉, 암호화 총칙 및 책임사항, 암호 관리 및 키관리에 있어서의 기본적인 권고사항만을 가이드하고 있다.

이 밖에도, DB 암호제품이 만족해야 할 국정원의 'DB 암호화 보안요구사항[5]', 개인정보보호법 및 개인정보의 안전성 확보조치 기준에 따라 고유식별정보 내부망 저장 시 암호화 적용여부 및 적용범위 결정을 위한 세부 기준을 안내하고 있는 안전행정부의 '개인정보 위험도 분석 기준 및 해설서[6]'와 금융보안연구원에서 발행한 'DB 암호화 최신동향 및 보안기술 분석보고서[7]' 등을 개인정보 및 DB 암호화 관련 선행연구 사례로 들 수 있을 것이다.

앞서 언급한 주요 가이드 및 지침의 경우 각각 개별적으로 DB 암호화 시 고려해야할 기준 및 세부 사항 등에 대해서 언급하고는 있으나, 그럼에도 불구하고, 암호화 적용 이전 단계부터 실제 암호화 적용 단계, 그리고 암호화 이후 운영 등의 각각의 단계에서 보다 구체적으로 고려해야 할 사항들에 대해서는 다소 부족한 실정인 것으로 판단된다.

III. DB 암호화 검증 프레임웍

3.1 개요

서론에서 언급한 바와 같이 DB 암호화 과정은 기업 규모에 따라 일부 차이가 있을 수 있으나 평문 상태의 데이터를 암호화 알고리즘을 통해 암호문으로 변환하는 식으로 진행되는 단순 시스템 변경 작업이 아닌 관련 법규 준수를 목적으로, 조직의 업무 프로세스 및 향후 관리 프로세스가 재설계 되어야 하는 복합 작업이다. 이에, DB 암호화의 기본 목적인 준거성을 달성하면서도 업무적 효율성 및 현실성 등을 고려해야 하는 어려움이 있다. 이러한 바를 충분히 고려하여 본 논문에서는 보다 체계적이고 현실적인 다음과 같은 DB 암호화 검증 프레임웍을 제시하고자 한다.

본 논문에서 제시하는 검증 프레임웍의 기본적인 외형은 한국정보화사회진흥원의 '정보시스템감리검증 프레임웍'[10]의 육면체 구조를 참조했음을 미리 밝혀두는 바이다. 정보시스템감리검증 프레임웍에서는 정보시스템의 유지보수 및 구축하는 정보화사업 유형에 따른 각 단계별 과정에 따른 감리 관점과 점검 기준을 제시하고 있다. DB 암호화 과정 또한 이러한 정보화사업과 유사하게, DB 암호화 적용 전에 영향평가 및 상관관계 검토를 위한 기획/분석 단계를 거쳐, 실제 암호화 적용이 일어나는 구축/개발/테스트 단계를 거치고 암호화 및 복호화가 발생하고 지속적인 관리 감독을 위한 운영 단계를 거치게 된다. 이에, 본 논문에서는 DB 암호화 과정 또한 정보시스템 감리 검증 관점에서 폭넓게 논의가 되어야 할 사안이라고 판단되어 해당 프레임웍의 기본 구조를 참조하고자 하였다.

그러나, 일반적인 정보시스템 감리와 DB 암호화 검증은 점검 기준 및 검증 방법에 있어서 상이한 부분

이 많은 것 또한 사실이기 때문에 암호화라는 상대적 특수성을 고려하여 본 DB 암호화 검증 프레임웍을 설계하였다.

DB 암호화 검증 프레임웍은 Fig. 1과 같이 암호화 적용 단계, 검증 관점, 검증 영역, 법률 및 기준의 네 가지 틀로 구성되었다.

다만, 실제 검증항목들이 도출되는 부분은 검증 영역 부분이며 이러한 검증 영역들은 법률 및 기준에 근거하며 각 항목들은 또한 어떠한 관점에서 검증할지에 대해 검증 관점들과 연계되어 있다.

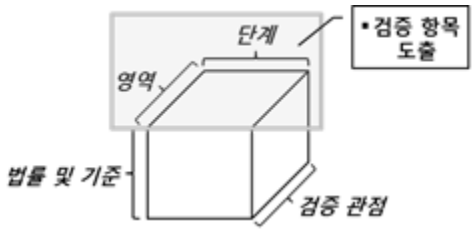

Fig. 1. The outline of DB Encryption Assurance Framework

3.1.1 "단계" 별 "검증 영역"

잘 알려져 있는 일반적인 정보보호 관리체계(ISMS)에서 흔히 운영과정 상 고려해야 할 요소는 보통 "Plan - Do - Check - Act"로 이루어져 있다. 이러한 점에 착안하여 본 검증 프레임웍의 "단계" 요소는 Check와 Act 영역을 한가지 단계로 포괄하여 [Fig. 2]와 같이 계획(Plan) - 적용 (Do) - 운영 (Check, Act)의 세가지 단계로 구분하여 각 단계별 검증 포인트를 제시하고자 하였다. "Check"와 "Act"의 과정을 하나로 묶어서 운영의 단계로 표현한 사유는 "Check" 과정에서 식별되는 암호화 및 복호화 관련한 중대한 이벤트들에 대해 즉각적인 Action plan을 세워 조직적으로 대응하여 암호화 관리상의 연속성과 안정성을 확보하고 있는지 검증하기 위함이다.

즉, 운영 단계에서 Check 이외에 Act 관점에서 검증 사항이 실제 암호화 관리 과정 상에 반영되고 있는지에 대해서도 검증하도록 한다.

앞의 암호화 검증 프레임웍 개요 부분에서도 언급한 바와 같이, DB 암호화 과정 또한, 정보시스템 구축의 일환으로서 관리감독이 필요한 사안이기 때문에 이러한 취지의 일환으로 단계별 검증 영역들을 다음과 같이 계획, 적용, 운영의 세 단계로 분류하였다.

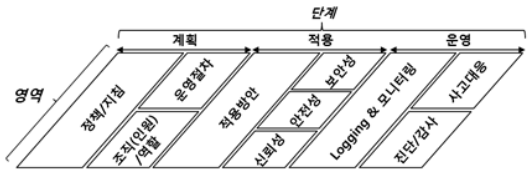

Fig. 2. The Assurance area of "each Phase"

- 계획 단계
  - 정책/지침, 조직(인원)/역할/운영절차 적용 단계
  - 적용방안, 신뢰성, 안전성, 보안성 운영 단계
  - Logging(로깅)&모니터링, 진단/감사, 사고대응

3.1.2 "법률 및 기준" 과 "검증 관점" 영역

앞서 언급한 단계 별 검증 영역에 대한 근거는 개인정보 암호화와 관련된 법률 및 아래 (Fig. 3)에서 보이는 바와 같이 현재까지 알려진 관계기관의 다양한 표준에 기반하고 있다.

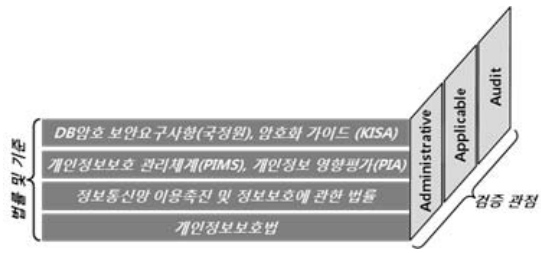

Fig. 3. The area of "Acts and Standards" and "Aspect of Assurance"

이러한 법률 및 기준을 토대로 개인정보 암호화에 따른 관리적 관점 (Administrative), 실 암호화 이행 시 적절성 및 현실성을 고려한 적용성 관점 (Applicable) 그리고 향후 운영 단계에서 주로 고려해야 할 감사 및 통제 관점 (Audit)의 세가지 측면을 검증 관점으로 제시하였다. 검증 관점은 3.1.1에서 언급한 단계 별 검증 영역에서 검증 항목들이 가져야 할 내적인 속성으로 DB 암호화 검증 시 검증자가 기본적으로 고려해야 할 요소로 이해할 수 있다.

3.2 DB 암호화 검증 프레임웍

3.1에서 언급한 네 가지 측면들을 종합하여 본 논문에서 제시하고자 하는 전체 DB 암호화 검증 프레임웍을 소개하면 [Fig. 4]와 같다.

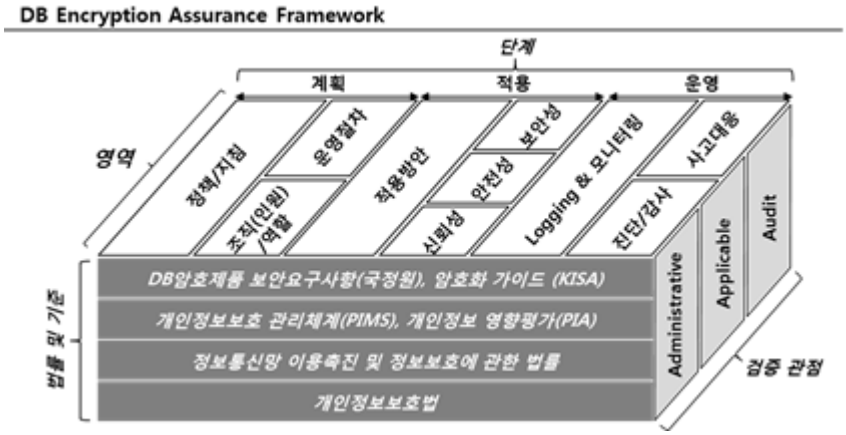

Fig. 4. The DB Encryption Assurance Framework

다시 말하자면, 본 DB 암호화 검증 프레임웍의 기본적 개념은 1) DB 암호화와 관련된 각종 법률 및 기준에 근거하여 2) DB 암호화 진행 시 거쳐야 하는 계획, 적용 및 운영 각 단계 별로 반드시 검토해야 할 주요 영역 및 검증 항목들을 도출하고 3) 이렇게 도출된 각 검증 항목들에 대하여 관리적 관점 (Administrative), 적용성 관점 (Applicable) 그리고 감사 및 통제 관점 (Audit)의 세가지 측면을 검증 관점으로 제시하는 것이라 할 수 있다.

IV. DB 암호화 검증 프레임웍 상세 내용

앞서 소개한 DB 암호화 검증 프레임웍은 구체적으로 어떠한 개별 검증 항목으로 구성되어 있으며, 이러한 검증 항목 기준에 대한 검토 시 검증자가 보다 고려해야 할 내용 들은 어떠한 것들이 있는지 본 장에서 중점적으로 다루어 보고자 한다.

4.1 "계획 단계" 검증 항목

DB 암호화 검증 프레임웍에서 제시한 바와 같이 계획 단계에서 검증해야 할 영역은 '정책/지침', '조직/역할', '운영절차'로 크게 나누어 볼 수 있으며 각 영역별 세부적으로 검증해야 할 항목에 대하여 구체적으로 살펴보도록 한다.

4.1.1'정책/지침' 내 검증 영역

정책/지침 내 검증 영역은 말 그대로 수범자의 DB

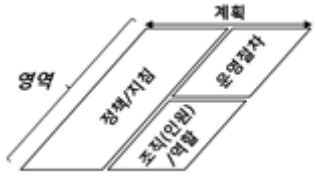

Fig. 5. The Assurance area of "Planning Phase"

암호화 적용에 필수적으로 선행되어야 할 암호화와 관련된 각종 기준[4]에 해당된다. 조직 내 수집, 보유 및 이용하고 있는 암호화 대상 개인정보를 우선 식별하고, 이러한 개인정보를 실제로 처리하고 있는 개인정보처리시스템 (편의 상 Database에 한정하도록 한다.) 및 해당 테이블(컬럼) 등을 확인하여야 한다. 이러한 현황 파악을 토대로 암호화 알고리즘 및 운영방식과 더불어, 조직의 개인정보처리시스템 환경에 적합한 구체적인 암호화 적용 방식을 선정하는 것 또한 필요하다.

뿐만 아니라, 말 그대로 암호화 적용에 있어 "핵심키" 역할을 담당하는 암호화 키 관리와 더불어, 이러한 키를 통해 복호화를 담당한 개인정보취급자에게 복호화 권한을 부여하는 부분 및 복호화에 대한 이력관리, 그리고 복호화 이력관리를 통한 이상 징후 탐지 시 사고여부를 확인할 수 있는 판단 기준 등에 대한 명시 또한 필요할 것이다.

아래는 이러한 정책/지침 내 검증이 필요한 검증 항목 및 고려요소 들에 대한 내용들이다.

1) 암호화 대상 개인정보
- 수집/이용되는 개인정보의 종류
- 법규 준수를 위한 최소 요건 암호화 적용
- 유출 사고 발생 시 피해 범위 최소화를 위하여 기타 개인정보를 포함한 암호화 적용

2) 암호화 대상 개인정보처리시스템 및 테이블
- 개인정보의 흐름 (Life-Cycle)에 근거한 개인정보처리시스템 종류
- 암호화 적용 대상 개인정보처리시스템 및 적용 테이블 현황

3) 암호화 알고리즘 및 운영 방식
- 안전한 양방향 암호화 알고리즘 (키 길이 포함) 및 운영 모드 선정
- 안전한 일방향 암호화 알고리즘(Hash 함수) 및 Salt 적용 방식

4) 암호화 적용 방식
- API 방식 / Plug-in 방식 / PIN 방식 등 업무 환경을 고려한 적용 방식 선정

5) 암호화 키 관리
- 암호화 키의 성격에 따른 Hierarchy(마스터 키 → 암호화키 등)분류
- 각 Hierarchy에 따른 암호화 키 생성, 사용 (보관 장소, 보관 방법, 암호화 적용), 폐기 (사용 주기 등) 및 복구 등

6) 복호화 권한 관리
- 복호화 권한 부여 기준 및 절차 명시
- 개인정보처리시스템 별 복호화 권한 필요자 (or 시스템 계정) 현황 관리

7) 복호화 이력 관리
- 복호화 이력 logging 및 향후 모니터링 방안
- 이상징후 탐지를 위한 모니터링 기준 제시

8) 사고 대응
- 이상 징후 탐지에 따른 사고 여부 판단 및 사고 대응 기준 명시
- 사고 시 피해 범위 최소화 및 복구 방안 제시

4.1.2 '조직(인원)/역할' 내 검증 영역

이 부분의 검증 항목들은 주로 일반적으로 우리가 쉽게 고려할 수 있는 DB 암호화와 관련된 책임과 역할 및 교육 등으로 구성하였다.

즉, DBA로 불리우는 DB 관리자와 암호화 관리자의 권한 분리와 DB 암호화와 관련된 유관 조직 및 인원간의 책임과 역할 (R&R: Rules & Responsibility), 암복호화 업무와 연관된 개인정보취급자에 대한 교육 등에 대한 검증이 필요할 것이다.

1) 권한 분리
- DB 관리자와 암복호화 관리자의 역할 및 권한 분리

2) 조직(인원) 간 R&R
- 복호화 권한 요청(신청)자 / 승인자 / 처리자 / 관리감독자 간 역할 및 책임 정의
- 향후 진단/감사 결과 도출된 이상행위자에 대한 처벌 및 조치를 위한 역할 및 책임 정의
- 사고로 판명된 경우, 관련 기관 신고, 내부 사고 조사, 소송 대응 및 홍보 등을 위한 역할 및 책임 정의

3) 암/복호화 권한 보유자 교육
- 권한 신청 절차 / 업무 상 필요한 최소한의 복호화 / 사후 모니터링 및 증빙

4.1.3 '운영절차' 내 검증 영역

운영절차 내 검증 영역은 앞의 4.1.1 및 4.1.2에서 각각 정의한 DB 암호화 정책/지침에 따른 주요 기준과 책임 및 역할에 따라 DB 암호화 적용 이후 운영 과정 상에서 반드시 필요한 운영절차 등으로 구성하였다. 가장 처음 신규로 DB 암호화 적용이 필요한 시스템 발생 시 또는 기존에 DB 암호화가 적용된 시스템이 업무적 사유로 인하여 변경이 필요할 경우에 대응하기 위한 절차를 고려해야 할 것이다. 또한, DB 암호화 이후 복호화에 대한 권한 관리를 위한 절차 및 이러한 복호화 이력에 대한 모니터링 절차, 이상 징후로 정의한 바에 의하여 사고로 의심되는 건에 대한 사고 대응 절차, 그리고 암호화 키의 Life-Cycle에 따른 관리 절차 또한 검증이 필요할 것이다.

1) 암호화 적용 대상시스템, 컬럼 변경관리 절차
- 개인정보처리시스템 신규 개발로 인한 암호화 적용 시 암호화 API 또는 Plug-in 적용에 따른 변경 관리 절차
- 기존 개인정보처리시스템 변경으로 인하여 암호화 대상 테이블(컬럼) 변경에 따른 변경 관리 절차

2) 복호화 권한 관리 절차
- 암호화 대상 테이블(컬럼)에 대한 복호화 요청 시 복호화 권한 부여 및 회수를 위한 절차

3) 복호화 이력 모니터링 절차
- 이상징후 탐지를 위한 모니터링 기준 및 절차

4) 사고 대응 절차
- 사고 시 피해 범위 최소화 및 법적 이슈 대응을 위한 절차

5) 암호화 키 관리 절차
- 암호화 키 Life-Cycle에 따른 관리 절차

4.2 "적용 단계" 검증 항목

암호화 적용 단계에서 검증해야 할 영역은 실제 DB 암호화 적용 과정 상에서 필수적으로 검토해야할 부분임에 틀림없다고 해도 과언이 아닐 것이다. 다만, 이 부분은 DB 암호화 적용이 필요한 조직의 업무적, 현실적, 그리고 시스템적 특징 등이 충분히 반영되어야 할 부분이라 일괄적으로 표준 항목을 정하기에는 다소 어려운 부분이 있는 것 또한 현실이다.

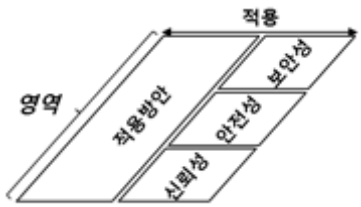

Fig. 4. The Assurance of "Application Phase"

이에 본 논문에서는 DB 암호화를 적용함에 있어서 누락되어서는 안되는 부분, 그리고 DB 암호화를 담당하고 있는 조직의 담당자 등이 간과하기 쉬운 부분 등에 대해서 DB 암호화 "적용 단계"의 검증 항목을 [Fig. 6]과 같이 '적용방안', '신뢰성', '안전성' 및 '보안성'으로 나누어 살펴보도록 한다.

특히, "적용 단계"의 검증 항목에 대하여는 반드시 현실적이고 실용적인 부분이 뒷받침되어야 함에도 불구하고 아직까지 이러한 DB 암호화 "적용 단계"에서 고려해야 할 구체적인 가이드나 기준 등은 부재한 실정이다.

4.1.1 '적용방안' 내 검증 영역

실제 기업의 개인정보처리시스템에 대한 암호화를 위해서는 성능 개선을 위한 CPU 및 메모리 업그레이드 뿐만 아니라, 암호화로 인한 DB용량 증설, 암호화 관련된 프로그램의 수정과 더불어 개인정보처리시스템을 사용하는 개인정보취급자의 업무프로세스에 걸친 다양한 사항에 대하여 고려하여야 한다. 물론, 본격적인 암호화 이전에 암호화 대상임에도 불구하고 불필요하게 개인정보처리시스템 내 보관되고 있는 개인정보에 대한 정리 작업 또한 필요하다. 이러한 과정을 거쳐 필요한 경우 암호화로 인한 관련 어플리케이션을 수정한다던가, 업무적 상관관계 등을 고려하여 주민등록번호의 경우 전체 13자리가 아닌 생년월일 부분을 제외한 주민번호 뒤 6~7자리를 부분 암호화 하는 등 관련 법규 상 허용되는 범위 내에서의 융통성 적용이 가능한 부분 또한 살펴봐야 할 것이다. 뿐만 아니라, 암호화로 인한 현업 업무 담당자의 업무가 곤란한 경우가 발생할 수도 있기에 이러한 영역까지 고려하여 '적용방안' 내 검증 영역을 도출하고 이에 맞는 대안을 수립하여야 한다. 물론, 본 절에서 다루고자 하는 부분은 규제 당국보다는 수범자에 해당하는 개인정보처리자 입장에서 보다 신경써서 고려해야 하는 항목 중의 하나라고 할 것이며 DB 암호화 적용 시 수범기관의 담당자로서는 반드시 짚고 넘어가야 할 사안이라고 하겠다.

1) 불필요 암호화 대상 개인정보 삭제
- 암호화 적용 시 암호화를 위한 최선의 선택은 암호화 대상 개인정보를 보유하지 않는 것임.
- 따라서, 업무적으로 또는 시스템 적으로 반드시 필요한 개인정보가 아닌 경우 또는 불필요하게 관리되고 있는 테이블 또는 컬럼 등에 대한 삭제 작업 선행
- 운영 시스템 뿐만 아니라, 테스트 및 개발 장비까지 포함

2) 개인정보처리시스템 별 암호화 적용 방식[7]
- 정책/지침에서 정의한 암호화 적용 방식을 우선적으로 반영하여 암호화 적용
- 어플리케이션 수정이 어려운 경우 Plug-in 방식을 통한 암호화 적용
- 기타 ERP와 같은 특수 패키지를 위한 PIN 방식, 또는 파일 암호화 방식 등에 대한 고려

3) S/W 수정[7]
- API 방식 또는 PIN 방식의 암호화 적용 시 암호화 대상 컬럼에 대한 암복호화 프로그램(API) 호출 고려
- 성능 개선, Index 검색 등의 사유로 인한 프로그램 수정 사항 고려
- 응용프로그램의 소스 수정 뿐만 아니라, 해당 DB query에 대한 최적화 고려

4) H/W (CPU, 메모리 및 저장 공간)의 증설
- Batch 프로그램 등을 통한 대량의 데이터에 대한 암복호화 일괄 처리 고려
- CPU 및 메모리 증설을 통한 일부 성능 개선 가능 여부 고려
- 암호화로 인한 암호화 저장 공간 및 암호화 대상 컬럼 증가에 따른 물리적 H/W 증설 고려

5) 부분 암호화
- 주민등록번호의 경우 업무상 부분 검색 등에 활용될 소지가 있음에 따라 시스템적으로 부분 암호화 적용 여부 고려
- 생년월일 6자리 또는 성별1자리 포함한 7자리 부분 암호화 적용
- 주민번호를 제외한 다른 필수 암호화 대상 개인정보의 부분 암호화 적용 불가 고려
- 전화번호 또는 주소 등에 대한 선택 암호화 적용 시 공통된 기준 및 적용방안 수립 필요함
  예1) 주소 컬럼 분리 후 시군구 동 이하 상세 주소 부분 암호화
  예2) 전화번호 컬럼 분리 후 국번 및 가운데 자리 이하 4자리 부분 암호화

4.2.2 '신뢰성(Reliability)' 내 검증 영역

본 절에서 다루고자 하는 '신뢰성'과 관련해서 필자가 표현하고자 하는 바는 필수 암호화 적용대상인 개인정보에 대해 DB 암호화를 적용함에 있어서 누락되는 요소가 없도록 꼼꼼하게 살펴보아야 한다는 점이다. 이처럼 암호화 대상이 누락되지 않기 위해서 살펴보아야 할 부분은 암호화 대상 개인정보의 흐름 분석을 통한 암호화 대상 개인정보처리시스템에 대한 확인도 필요하지만, 식별된 개인정보처리시스템 내 관리소홀 또는 업무 담당자의 편의 등을 이유로 암호화 대상 개인정보가 평문 형태로 존재하지 않는지 또한 반드시 점검하여야 한다.

1) 암호화 대상 시스템 현황 분석
- 암호화 대상 개인정보의 흐름 분석을 통해 암호화 대상 시스템에 대한 정확한 분석 필요
- 시스템 담당자 인터뷰, 시스템 실사 및 필요 시 소스 검토를 통한 대상 시스템 파악
- DBMS 이외에도 시스템 간 로그 (특히 기업 내부의 데이터 공유를 위한 연계시스템 로그) 및 정기적으로 생성되는 일괄처리형 파일 등에 암호화 대상 개인정보가 존재하는지 확인 필요
- 특히, 주로 누락되는 개발 및 테스트 환경에 대한 확인 필요

2) 시스템 내 테이블 및 컬럼 조사
- 암호화 대상 시스템 현황이 도출되면 해당 시스템 내 어떤 테이블의 어느 컬럼을 암호화해야 하는지 조사 필요
- 상용 암호화 툴을 사용하였을 경우 안정화 등의 사유로 원본 테이블 및 컬럼을 변경하여 보관하는 경우에 대한 확인 필요
- 시스템 개발이 오래되었거나, 관리 소홀로 인한 개인정보 보유 컬럼 확인이 어려운 경우에 대한 전수 검사 검토
  예1) DB 관리자가 수작업으로 검토
  예2) DB 내 보든 테이블에서 2~30개의 레코드(row) 추출 후 개인정보 암호화 대상 여부에 대한 패턴 검색

4.2.3 '안전성(Safetiness)' 내 검증 영역

본 절에서는 KISA의 암호 알고리즘 및 키 길이 이용 안내서[2]와 같이 DB 암호화 시에 사용된 일방향 또는 양방향 암호화의 선택이 올바른지, 그리고 양방향 암호화 적용 시 올바른 암호화 모드를 사용하였는지에 대하여 검증하는 영역이다. 다만, [2]에서는 일방향 암호화 알고리즘 적용 시 보다 안전한 암호화 값(해쉬 값) 생성을 위한 부분은 언급하고 있지 않아 본 논문에서는 이 부분에 대해서도 일부 내용을 추가하고자 한다.

1) 암호화 알고리즘의 올바른 사용
- 암호화에 사용된 알고리즘이 안전성이 증명된 알고리즘이 사용되었는지 확인
- 암호화된 데이터의 샘플링을 통하여 암호화 round 수 및 키 생성 알고리즘 등에 대한 검증
- 또한, mode of operation이 안전한 모드를 사용하고 있지는 않은지에 대한 확인

2) 일방향 암호화 알고리즘
- 일방향 암호화 대상 개인정보인 비밀번호의 경우 같은 비밀번호를 사용하는 사용자의 비밀번호에 대한 일방향 암호화 시 같은 해쉬 값이 생성되지 않은지에 대한 확인
- 해쉬값이 유출되어도 안전할 수 있도록 시스템 내부 salt 값을 추가하였는지 확인

- 그럼에도 불구하고 해독을 어렵게 하기 위해 해쉬 횟수 추가 여부 등 확인

4.2.4 '보안성(Security)' 내 검증 영역

최근들어 사용자 편의성 및 시스템 접근성을 향상시키기 위하여 DB 암호화 관리자 시스템을 웹 기반으로 개발하는 경우가 상당하며 이에 따라 암호화 관리자 시스템의 안전성, 접근통제, 권한 부여 이력관리 등을 보다 더 세밀하게 살펴보아야 할 필요가 있다. 또한 상용 DB 암호화 업체들도 일반적인 어플리케이션 개발 시 적용되는 웹 개발 보안 항목 등을 반드시 준수하여야 함에도 불구하고 이 부분에 대해 일부 미흡한 부분이 있어 DB 암호화 시스템의 자체적인 보안성에 대한 검증도 반드시 필요한 영역의 일부라 하겠다.

다만, 일반적으로 고려해야 할 어플리케이션에 대한 보안 점검 부분에 대한 전부를 언급하는 것은 본 논문의 취지와 일부 어긋나는 바가 있어 DB 암호화 검증 프레임웍 관점으로 바라보았을 때 필요한 최소한의 항목들에 대해서만 언급하도록 한다.

1) 접근통제
- 암호화 관리자 페이지에 대한 외부망을 통한 원격접속 여부 확인
- DB 암호화 관리자 시스템에 접근 가능 PC를 윈도우의 원격데스크탑 등을 통한 2차 접근 가능 여부 확인
- DB 암호화 관리자 시스템에 대한 접근하는 IP 또는 MAC 기준 접근 통제 여부 확인
- 중복 로그인 차단 및 세션 로그아웃 설정 여부
- 로그인 시 최종 접속 기록 표시 여부
- 장기 미접속 계정의 계정 잠금 여부
- 부여받은 권한 이외의 시스템 보안 취약점을 통한 권한 우회 차단 여부
- 네트워크 통신구간 암호화 적용 여부

2) 비밀번호 관리
- 개인정보보호법 및 정보통신망법 기준 개인정보처리시스템의 비밀번호 설정 기준 준수
- 최초 접속 시 비밀번호 강제 변경 여부
- 비밀번호 변경주기 설정 여부
- 비밀번호 실패횟수 설정 및 횟수 초과 시 계정 잠금 여부
- 비밀번호 분실 시 랜덤방식으로 초기화 하여 전송 후 재접속 시 비밀번호 재설정 여부

3) 사용이력 관리
- 시스템 로그인, 데이터 복호화, 조회/수정/출력/다운로드 등 제반 개인정보 취급행위 로깅
- 최상위 관리자 (Admin)의 복호화 계정 생성, 복호화 권한 부여 등 시스템 운영 행위 로깅
- 해당 이력에 대한 수정/삭제 행위 차단 및 무결성 보장 방안 (WORM 디스크 활용)
- 관련 법규에 따른 로그 보관 및 백업 여부

4.3 "운영 단계" 검증 항목

마지막으로 암호화 운영 단계에서 검증해야 할 영역은 암호화 작업 이후 실제 시스템 및 사용자들로 인해 발생하는 복호화 이력에 대한 'Logging & 모니터링', '진단/감사' 및 '사고대응'과 관련된 영역에 대해 살펴보아야 할 것이다.

Fig. 5. The Assurance of "Operation Phase"

뿐만 아니라 계획 또는 적용 단계와는 달리 암호화 이후 실제 운영 단계임을 감안하여 해당 영역별 검증 항목에 대하여 실제적으로 진행되고 있는 사항들에 대한 증빙자료 또한 확인이 필요할 것으로 보인다.

4.3.1 'Logging & 모니터링' 내 검증 영역

개인정보취급자 및 DB 암호화 관리자의 복호화 이력과 더불어 시스템에서 발생하는 복호화 로그를 어느 수준으로 남기고 이를 모니터링할 것인지에 대하여 현실적인 고민이 필요하다. 그러한 이유는 특히, 일반적으로 시스템에서 발생하는 복호화 이력은 그 양이 상당하기에 대부분의 기업에서는 해당 로그를 남기지 않는 경우가 많으나, 이러한 경우 사고 예방을 위한 모니터링 및 사고 발생 시 추적이 곤란하기 때문에 대량의 일괄처리형 작업의 경우는 로그를 남기지 않고 이외에 개인정보처리자가 시스템에 로그인하여 개인정보를 취급(복호화)하는 경우에 대해서만 로그를 남기

는 방안을 검토해야 한다. 또한 시스템을 통해 로그를 남기는 경우, 해당 사용자에 대한 추적이 가능하도록 시스템 로그인 정보와 복호화 로그를 연계하여 관리하는 방안 또한 검토해야 한다. 물론 DB암호화 관리자가 DB에 직접 접근하여 복호화를 하는 경우는 로그를 남기는 방안을 검토해야 한다.

이러한 관점에서 Logging & 모니터링' 시 검증해야 할 부분은 로그를 남겨야 할 이벤트, 즉 로그를 남겨야 할 기준에 대하여 타당하게 설정하고 적용하고 있는지에 대한 부분부터 각각의 개인정보처리시스템 간의 로그 분석을 위한 정형화된 템플릿(로그 수집 항목 및 데이터 형식 등에 대한 통일)을 마련하고 있는지와 이러한 로그들의 상관관계 분석을 위한 모니터링 여부 등에 대한 검증이 필요하다고 할 것이다.

1) logging 기준 수립 및 적용
- 개인정보취급자와 개인정보처리시스템으로 분류 후 개인정보취급자의 DB 직접 접근을 통한 복호화 이력 100% 로깅
- 개인정보처리시스템의 경우 일괄처리형 작업에 한하여 로그를 남기지 않는 방안 검토

2) logging 템플릿 활용
- 시스템간 로그 표준을 수립하여 동일하게 적용하고 있는지에 대한 확인
- 5W1H 기준 향후 tracking이 가능한 로그 표준 수립 여부 확인
  예) 누가(취급자 ID)/언제(복호화 시간)/어디서(취급자 IP)/무엇을(누구의 정보를)/왜(무슨 업무로)/어떻게(시스템 명) 등의 이력이 남도록 관리

3) 효율적 모니터링을 위한 이상 징후 기준 수립 및 적용
- 조직의 개인정보 취급업무의 특성 및 근무 환경 등을 고려한 복호화 이상 징후 정의
- 이상 징후에 해당하는 경우 다음 절에서 다룰 진단/감사 조치를 취하고 있는지 확인

4.3.2 '진단/감사' 내 검증 영역

'진단/감사' 내 검증 영역은 5.1.1의 'Logging & 모니터링'을 통해 식별된 이상행위 또는 내부 또는 외부 감사 수행시 위반사항으로 도출된 부분에 대한 개선 등의 조치가 수행되는지에 대하여 검증이 필요한 부분이다.

1) 진단/감사 기준 정의 및 적용
- 개인정보 복호화 권한을 보유한 모든 개인정보취급자 (시스템 포함)로 정의
- 상시 진단은 복호화 이력에 대한 모니터링을 통해 이상 징후 발견 시 해당 이상 징후자 및 시스템에 대한 검증 수행
- 정기 감사는 본 논문에서 언급하고 있는 개인정보 암호화와 관련된 제반 영역에 대한 현황관리 상태를 검증하는 것을 목표
- 단, 감사 대상을 특정 시스템, 특정 개인정보취급자로 국한하여 진행하는 방안도 고려

2) 진단/감사 이행 및 조치
- 이상징후의 탐지 및 알람 여부
  예) 시스템에서 자동으로 진단/감사 역할을 수행하는 진단자(감사자)에게 SMS 또는 이메일 등으로 처리
- 이상징후 접수 시 조치 방안
  예) 진단자(감사자)는 이상징후자와의 인터뷰 및 실사 (PC 및 네트워크 사용이력 등)를 통해 실제 사고와 연관되는 사항인지, 기존 개인정보 취급업무와의 연장선상인지 확인 필요
- 개인정보취급자의 단순 부주의 또는 사안이 경미할 경우 조직의 내부 사규에 따라 주의 또는 경고 등의 조치 방안
- 진단/감사 이력 관리 및 인식제고를 위한 홍보 방안

4.3.3 '사고대응' 내 검증 영역

사고대응과 관련한 검증 영역은 기 구축된 사고대응 기준 및 사고대응 절차에 따른 지속적인 사고대응 관리 체계가 수립되어 있는지와 이러한 체계에 기반하여 DB 암호화 작업 이후 올바르게 사고대응을 수행하고 있는지 등에 대하여 검증하여야 할 것이다.

1) 초기 대응 체계 수립 여부
- 사고대응절차 및 기준에 따른 초기 비상 대응 매뉴얼 마련 여부
- 사고 경위 조사부터 언론, 관계당국, 소송 등에 대응하기 위한 전담 TFT 구성 여부 확인
- 사고 경위 분석 및 향후 소송 대응 등을 위한 전자 증거 수집 및 보존
- 개인정보 유출사고로 판단될 경우 관련 법령에

따라 유관기관에 신고 및 정보주체에 통보
- 외부 전문가 그룹과의 협업체계 유지

2) (사고 발생 시) 실 사고대응 이력
- (필요 시) 외부전문가 그룹의 도움을 받아 사고 경위에 대한 전반적인 조사 진행 체계
- 외부자의 침입을 통한 시스템 해킹인지, 내부 개인정보취급자의 정보유출인지 확인 체계
- 회사의 관리/감독 소홀 또는 개인정보 보호조치 위반으로 인한 사고발생인지에 대한 상세 사고 원인 및 경위 분석 체계
- 사고 관련 증거 수집 및 대응 논리 체계
- 내부 인원에 의한 사고인 경우 해당 사고자에 고소/고발 등 처리 방안
- 대내/외 홍보 및 언론 추이 분석 및 대응
- 사고로 인한 피해범위 최소화를 위한 후속조치 계획 수립 및 착수

3) 모의 사고대응 훈련
- 신속하고 효과적인 사고 대응체계 유지를 위한 정기/수시 모의 사고대응 훈련 진행 체계

V. 결 론

지금까지 본 논문에서는 별첨 〔표 1〕과 같이 DB암호화 각 단계별 검증해야 할 영역을 분류하고 이에 따른 세부 검증항목들을 정의하였다. 표에서 보여지는 바와 같이, DB 암호화 관점에서 현재까지 진행된 제반 선행 연구에서는 기존에 다루지 않았거나, 다루더라도 일부 언급이 부족한 영역에 대하여 보다 체계적이고 실무적인 시각에서 다루고자 노력하였다.

본 논문에서 제시하는 이러한 DB 암호화 검증 프레임웍을 통하여, 개인정보처리자 즉, 수범자 관점에서는 개인정보를 암호화함에 있어서 보다 안전하고 효율적인 관리체계를 수립하고, 관계기관 및 행정당국 관점에서는 개인정보처리자들이 실제 제대로 개인정보를 암호화하였는지 검증할 수 있는 상호간의 기준 및 근거가 되기를 바란다.

다만, 본 논문의 암호화 검증 프레임웍의 모든 영역에 대해서 일률적으로 모든 기업에게 개인정보 DB 암호화 검증 기준을 만족하도록 요구하는 것은 현실적으로 어려움이 따를 것으로 보인다. 기업의 규모와 IT 업무 환경을 적절하게 고려함과 동시에 법률 요구사항을 충족할 수 있는 선에서 수범자 및 개인정보 보호 규제 당국간의 합리적인 협의점에 대해 보다 심도깊은 논의를 진행하는 것 또한 한편으로는 필요할 것으로 보인다.

References

〔1〕 KISA, "The Guide to Using Encryption," 2010. 01
〔2〕 KISA, "The Guide to Using Cryptographic Algorithm and Key Sizes," 2010.01
〔3〕 KISA, "The Guide to Managing of Private Information DB Encryption," 2010.01
〔4〕 KISA, "The Guide to Establishment of Encryption Policy in order to Protect IT Information Assets of Company," 2010.01
〔5〕 NIS, "Security Requirements for DB Encryption Product," 2010.04
〔6〕 KISA, "The Guide and Standard of Private Information Risk Analysis," 2012.03
〔7〕 FSA, "The Technical Analysis Report of Recent Trend DB Encryption and Security Technique," 2012.09
〔8〕 Ministry of Government Legislation, http://www.law.go.kr, Act on Promotion of Information and Communication Network Utilization and Information Protection
〔9〕 Ministry of Government Legislation, http://www.law.go.kr, Personal Information Protection Act
〔10〕 NIA, "The guide of Information System Audit and Check," V2.0, 2007.2

〔※별첨〕

Table. 1. A Detail Assurance Article of DB Encryption Assurance Framework

단계	영역	본 논문 제시 검증 항목 상세 영역	現 선행 연구 사례*	필수/옵션** (M/O)	검증 관점		
					Admin	Applicable	Audit
계획	정책/지침	1) 암호화 대상 개인정보	●	M	✓	✓	
		2) 암호화 대상 개인정보처리시스템 및 테이블(컬럼)	●	M	✓	✓	
		3) 암호화 알고리즘 및 운영 방식	●	M	✓	✓	
		4) 암호화 적용 방식	●	M	✓	✓	
		5) 암호화 키 관리	◐	M	✓		
		6) 복호화 권한 관리	◐	M	✓		✓
		7) 복호화 이력 관리	○	M	✓		✓
		8) 사고 대응	○	M	✓		✓
	조직(인원)/역할	1) 권한 분리	◐	O	✓		✓
		2) 조직(인원) 간 R&R	◐	O	✓		✓
		3) 암/복호화 권한 보유자 교육	○	M	✓		✓
	운영절차	1) 암호화 적용 대상시스템 및 컬럼 변경관리 절차	○	M	✓	✓	
		2) 복호화 권한 관리 절차	◐	M	✓		✓
		3) 복호화 이력 모니터링 절차	◐	M	✓		✓
		4) 사고 대응 절차	◐	M	✓		✓
		5) 암호화 키 관리 절차	●	M	✓	✓	✓
적용	적용방안	1) 불필요 암호화 대상 개인정보 삭제	○	O	✓	✓	
		2) 개인정보처리시스템 별 암호화 적용 방식	○	O		✓	
		3) S/W 수정	○	O		✓	
		4) H/W (CPU, 메모리 및 저장 공간)의 증설	○	O		✓	
		5) 부분 암호화	○	O	✓	✓	
		6) 업무 프로세스의 변경	○	O	✓	✓	
	신뢰성	1) 암호화 대상 시스템 현황 분석	○	M	✓	✓	
		2) 시스템 내 테이블 및 컬럼 조사	○	M		✓	
	안전성	1) 암호화 알고리즘의 올바른 사용	●	M		✓	
		2) 일방향 암호화 알고리즘	◐	O		✓	
운영	보안성	1) 접근통제	●	M	✓	✓	✓
		2) 비밀번호 관리	●	M	✓	✓	✓
		3) 사용이력 관리	●	M	✓	✓	✓
	Logging/모니터링	1) logging 기준 수립 및 적용	◐	M	✓		✓
		2) logging 템플릿 활용	◐	O	✓		✓
		3) 효율적 모니터링을 위한 이상징후 기준 수립 및 적용	○	O	✓		✓
	진단/감사	1) 진단/감사 기준 정의 및 적용	○	O	✓		✓
		2) 진단/감사 이행 및 조치	○	M			✓
	사고대응	1) 초기 대응 체계 수립	◐	O	✓		✓
		2) 사고대응	◐	M			✓
		3) 모의 사고대응 훈련	◐	O	✓		✓

* ●: 사례 양호, ◐: 일부 사례 존재, ○:사례 미흡 ** 개인정보보호 관련 법규 기준 필수/옵션으로 구분

〈저자소개〉

고 영 대 (Young-dai Ko) 정회원
2004년 8월: 고려대학교 정보보호대학원 정보보호학과 석사
2013년 2월~현재: 법무법인(유) 율촌 전문위원
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 개인정보보호, 정보보호, 디지털 포렌식, 대칭키 암호

이 상 진 (Sang-jin Lee) 종신회원
1989년 2월 ~ 1999년 2월 : 한국전자통신연구원 선임 연구원
1999년 2월 ~ 2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월 ~ 현재 : 고려대학교 정보보호대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 디지털 포렌식