Journal of The Korea Society of Computer and Information
Vol. 22 No. 6, pp. 41-48, June 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.06.041

Study on video information regulation and VPIC compliance issues in GDPR

Ki-Il Ryu*, Young-Im Cho**

Abstract

All the personal information controllers or processors collecting, processing and storing personal information through the entry into force of the EU GDPR (General Data Protection Regulation) are required to provide the basic principle of privacy by design at all stages of developing products or services throughout the organization, And to ensure that the basic rights of the subject of personal information are protected and that internal control techniques are provided to prevent any abuse or leakage. We will review the regulations and countermeasures required by the GDPR for video information with serious privacy problems, and propose a solution.

▸Keyword: EU, GDPR, DPO, Video Information, Forensics, Internal Control, PbD, VPIC, CCTV, VPM

I. Introduction

오늘날에는 CCTV를 빼고 방범을 말 할 수 없을 정도로 도시, 시골 할 것 없이 CCTV가 설치 운용되고 있다. CCTV 설치는 단지 영상방범 모니터링에만 국한되는 것이 아니라 개인영상정보의 생성과 저장이 동시에 이루어지는 것이며, 사건사고 발생 시 증거자료 활용을 위해 디지털 포렌식 절차에 따라 합법적으로 제공하게 되지만, 유출시 개인의 민감한 사생활이 공개되는 침해상황으로 이어지게 된다.

국내에서는 2011년부터 시행된 개인정보보호법에서 영상정보의 특수성과 민감성을 인정하고 영상정보처리기기의 접속정보를 별도 보관하고, 저장된 영상의 위변조를 방지하여야 하며, 처리자에 의한 오남용과 유출을 방지하기 위한 대책으로 내부통제시스템을 구축하도록 하고 있다[1,2].

지방자치단체에서 각 목적별로 분산 관리되던 CCTV의 통합운영을 위한 CCTV 통합관제센터에서 발생되는 국가기관에 의한 투명한 영상관리 여건 보장과 근무자에 의한 사생활 침해 방지 기술적 조치 요구가 대두되었고[3,4], 최근에 들어 이러한 문제점이 개인정보보호법에서 요구되어 지는 컴플라이언스 이슈에 대응하는 VPM 기술들이 도입되고 있다.

CCTV 시장은 국내는 물론이고 전 세계적으로 중국이 가격과 기술력으로 앞서 있어, 해외에서 국내 제품들이 고전을 면치 못하고 있는 상황에서 2016년 제정된 유럽의 GDPR(General Data Protection Regulation) 즉 일반정보보호규정은 국내 CCTV 제조사에게 큰 위협이면서 기회이다.

왜냐하면 개인정보 처리자는 개인정보가 안전하고 투명하고, 적법하게 처리되도록 관련 조치를 하여야 하고, 독립적인 지위의 정보보호책임관이 이를 관리 감독하게 하여 법 위반 시 감독관청에 즉각 보고의 의무를 규정하고 있기 때문이다. 위반 시 상상을 초월하는 벌금을 부과할 수 있게 하고 있어, 개인정보처리자나 정보보호책임관은 법을 위반하지 않기 위해 법의 규정을 충족할 수 있는 CCTV제품을 요구하고 사용하게 될 것이 명확하기 때문에 관련 기술을 적용한 제품이 우선적으로 사용될 것이다.

2018년 시행을 앞두고 있어 본 논문에서는 GDPR에서 요구하는 규정을 분석하여 국내 CCTV 제조사들이 해외에서 경쟁력을 갖추어 새로운 기회를 잡도록 관련 기술을 제시하고자 한다. 본 논문의 구성은 II장에서는 GDPR의 개요를 설명하고, III장에서 GDPR에 대한 대응기술을 제안한 후 IV장에서 영상정보처리기기에서의 대응기술 분석과 적절한 대응기술을 제시하고, V장에서 결론을 맺고자 한다.

• First Author: Ki-Il Ryu, Corresponding Author: Young-Im Cho
*Ki-Il Ryu (kikiyoo@daum.net), Dept. of Computer Science, Gachon University
**Young-Im Cho (yicho@gachon.ac.kr), Dept. of Computer Science, Gachon University
• Received: 2017. 05. 16, Revised: 2017. 06. 05, Accepted: 2017. 06. 20.

II. Overview of GDPR

1. What is GDPR?

EU는 2015년 12월 15일 GDPR을 합의하고, 2016년 4월 6일 최종안을 발표, 2016년 4월 24일 유럽의회를 통과하여, 2016년 5월 4일 Official Journal을 공표, 2016년 5월 24일 발효되었다. GDPR의 규제 범위와 내용이 방대하여 그 시행을 2년 유예하여, 2018년 5월 25일에 시행하도록 하였다[5].

① 총칙

GDPR은 개인정보의 처리에서 자연인 보호에 관한 규칙 및 개인정보의 자유 이동에 관한 규칙을 규정하고, 자연인의 기본적 권리와 자유, 특히 개인정보의 보호권을 보호하고, EU내 개인정보의 자유로운 이동은 개인정보에 대한 자연인 보호 관련의 이유로 제한되거나 금지되지 아니하도록 하였다.

② 적용대상 및 구성요소

EU 국민의 개인정보(personal data)를 EU내 또는 역외에서의 처리하는 모든 경우에 적용되며, 개인정보는 신원을 식별하거나 식별 가능하게 하는 개인에 대한 모든 정보로서 성명, 식별번호, 위치자료, 온라인 ID, 이메일, 영상이나 사진 등과 같은 식별자 또는 신체적, 생리학적, 유전적, 정신적, 경제적, 문화적, 사회적으로 그 개인을 식별 가능한 하나 이상의 요인들의 참조에 의하여 직간접적으로 식별 가능한 자료로 정의된다. 또한 처리에 대한 정의로 개인정보에 행해지는 모든 조작으로 수집, 기록, 구조화, 저장, 개조 또는 변형, 회수, 사용, 전송에 의한 공개, 파급 또는 다른 방법으로 이용가능화, 정렬 또는 조합, 제한, 삭제 또는 파괴 등 자동화 수단을 불문하고 개인자료 또는 개인자료군에 대해 수행되는 모든 작업 또는 작업군을 의미한다.

통제자(controller)는 단독으로 또는 공동으로 개인자료 처리의 목적과 수단을 결정하는 자연인 또는 법인, 공공당국, 기관 또는 기타 조직을 의미한다.

처리자(processor)는 통제자를 대신하여 개인자료를 처리하는 자연인 또는 법인, 공공당국, 기관 또는 기타 조직을 의미한다.

감독관청(supervisory authority)은 제51조에 따라 회원국이 설립한 독립적 공공관청을 의미한다.

정보보호책임관(data protection officer)은 개인정보 처리에 따른 내부적 규정준수를 관리하는 자로, 기존 Compliance Officer와 유사하나 동일하지 않으며, 이사회가 아니라 감독관청 규제관의 의해 감독되어지도록 하고 있다. 이는 독립적 업무를 수행할 수 있도록 법적 지위를 보장하여 통제자 및 처리자에 의한 부적절한 개인정보 처리 위반 발생 시 지체 없이 감독관청에 통지할 수 있게 하고, 그에 따른 법적 의무를 지게 하기 위해서다.

국가간 처리(cross-border processing)는 통제자나 처리자가 하나 이상 회원국에 설립된 경우, 그 하나 이상 회원국에서 설립활동과 관련하여 발생하는 개인정보를 처리하거나, 통제자나 처리자가 하나의 설립활동과 관련하여 발생하지만, 하나 이상 회원국의 정보주체에게 실질적 영향을 줄 것 같은 개인정보의 처리를 말한다. 이는 중요한 의미로 EU 회원국의 소속과 상관없이 EU 회원국의 국민의 개인정보를 처리하게 되는 통제자 또는 처리자에게 영향을 미친다는 원칙으로, 최근 클라우드 CCTV 등 인터넷을 통한 영상 전송 및 저장 관리 서비스나 제품이 출시되고 있는데 이 또한 규제를 받게 된다.

2. Main contents

① 개인정보의 합법적, 공정, 투명한 처리

개인정보 통제자 및 처리자는 개인정보 수집시 정당성, 필수불가결성과 보관 및 처리시 정확성, 보관기한 제한, 무결성 및 기밀성 등 합법적이고 공정하며, 투명한 방식으로 처리하도록 책임을 요구하고 있다.

② 정보주체의 기본권적 권리

정보주체는 개인정보에 대하여 통제자 및 처리자로부터 수집고지권, 권리고지권, 접근권, 정정권, 잊혀질권리, 처리반대권, 정보이동권, 프로파일링 반대권 등 정보주체자로서 주체적이고 능동적인 기본권을 부여하고 있다.

③ Data protection by design and by default

상품이나 서비스를 개발하는 모든 공정에서 개인정보보호를 고려한 시스템 공학적 접근을 해야 한다는 원칙으로, 기존 Privacy by design and by default라는 원리와 같으며, GDPR 전체에 기본이 되는 대 원칙중 하나다.

④ 처리자 및 통제자의 책임

정보주체자가 정보주체권을 행사시에 통제자 및 처리자는 응할 의무와 규정 위반에 대한 위반통지의무, 정보보호 영향성 평가, 정보보호책임관(Data Protection Officer: DPO)을 선임할 책임을 명시하고 있다.

⑤ 위반 시 제재

위반에 대하여는 일반 위반 시 전년도 매출액의 2% 또는 1천만유로 중 큰 금액의 벌금, 중대 위반 시 전년도 매출액의 4% 또는 2천만 유로 중 큰 금액을 벌금을 내도록 하고 있다[6].

III. Response technology proposal for GDPR

본 절에서는 GDPR의 도입을 앞두고 발생할 수 있는 개인정보보호의 기술적 미비와 컴플라이언스 이슈 부적합에 따른 제품의 경쟁력 저하 등 문제점들을 사전에 방지하고자 GDPR 규정내 여러 조항 중 발생할 수 있는 문제점들과 관련된 중요 규제조항을 분석하여 그에 따른 적절한 대응기술을 제시하고자 한다.

1. Comparison of domestic Privacy Protection Act with GDPR

GDPR에서 규정한 개인정보의 범위는 광범위하고 포괄적이어서, 문맥, 이론, 기술, 가이드라인, 실 적용례 등으로 해석해야 하며 우리나라 개인정보보호법의 개인정보의 범위와 유사하다.

본 논문에서는 이러한 맥락에서 GDPR과 개인정보보호법의 몇 가지 비교하여 제시하고자 한다.

첫째 개인보호 대상의 정의관점에서 두 개념은 유사하다. GDPR에서 처리에 대한 정의를 영상에 맞게 보기 위해서 우리나라 개인정보보호법 및 개정안 등의 처리 정의를 보면 촬영, 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 인쇄, 화면표출, 정정, 복구, 이용, 제공, 공개, 파기, 삭제, 확대, 축소, 방향이동, 로그기록, 전자지문 생성, 비식별화, 차폐(遮蔽), 그밖에 이와 유사한 행위로 볼 수 있다고 하였다[7].

둘째 GDPR의 통제자 또는 정보보호책임관(DPO)이 개인정보보호책임자와 유사하며 책임과 역할 또한 유사하다. 통제자 또는 DPO는 처리자에 의해서 처리되는 영상에 대하여 보호 계획의 수립 및 시행, 처리 실태 및 관행의 정기적인 조사 및 개선, 처리와 관련된 불만의 처리 및 피해 구제, 유출 및 오남용 방지, 보호 교육 계획의 수립 및 시행, 개인정보 보호 및 관리·감독으로 볼 수 있다 따라서 두 개념상 개별적 용어의 사용과 흐름만 다를 뿐 일맥상통한다.

셋째, 국내법에서는 개인정보보호책임자의 보호책임과 의무를 이행하기 위한 핵심으로 내부통제기술을 적용한 시스템 구축을 의무화 하고 있다. VPM(Video Privacy Management) 또는 VPIC(Video Privacy Internal Control) 기술을 규정하고 있다. 처리자의 처리 행위 전반에 걸쳐 상세한 로그기록을 생성하여 보관하고, 저장영상의 위변조 방지를 위해서 전자지문(해시값)을 생성 관리하며, 유출 방지를 위해서 시스템을 통한 반출관리를 요구하고, 정보주체자의 정보 제공요청시 제3자의 익명성 보장을 위해 비식별화 즉 제3자의 얼굴의 마스킹을 하도록 하고 있다.

국내 개인정보보호법에서 규정한 주요 조항을 그림으로 나타내면 Fig.1과 같다. 영상정보처리기기를 설치 및 운영 시 설치 목적과 맞게 영상을 촬영하여 수집하여야 하며(법 제15조, 제25조), 처리 목적이 완료 또는 파기 요청 정보에 대하여는 안전한 파기(법 제21조), 민감한 고유식별정보에 대한 분실 · 도난 · 유출 · 변조 · 훼손에 대한 안전성 확보(법 제24조), 접속기록 보관(법 제29조), 개인정보의 훼손 · 멸실 · 변경 · 위조 · 유출 방지(법 제50조) 의무가 있다. 이러한 규정은 이후에서 살펴볼 GDPR의 규제조항과 유사하다.

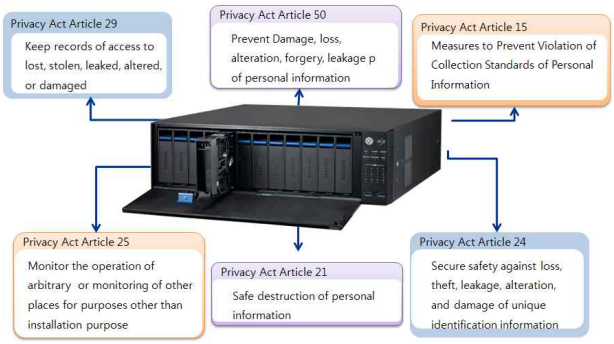

Fig. 1. Main Provisions of Personal Information Protection Act[8].

2. Regulatory response technology

앞서 제시한바와 같이 GDPR은 개인정보주체의 권리 및 통제자와 처리자의 의무를 규정하고, DPO에 의한 정량적 감사관리 및 내부적 규정준수 분석이 가능한 기술이 요구하고 있어, GDPR 컴플라이언스에 대응하는 기술이 적용된 CCTV 및 저장장치 등의 영상정보처리기기가 필요하다.

GDPR 컴플라이언스 관련 규정에 대하여 영상에 대한 요구기능과 관련 기술을 분석하여 본 논문에서는 아래 Table 1과 같이 요약하여 제안한다. 이것은 GDPR 규정에서 영상정보의 처리에 대한 요구 기능을 분류하고 적용할 기술을 이해하는데 의미 있는 표이다. 이 표에서 GDPR의 각 조항별 중요 요구 기능을 보면, 제30조의 처리행위의 기록, 제32조의 보안적 처리, 제33조의 위반사실 통지, 제15조의 개인정보 열람권, 제25조의 전주기 디폴트 데이터 보호 조치, 제28조 통제자에 의한 감사, 제5조 개인정보 처리의 원칙, 제6조 처리의 정당성, 제17조 잊혀질 권리를 규정하고 있다.

Table 1. GDPR Compliance Issues

Regulation	Function	Method
Records of processing actions (§ 30) (Processor, processing purpose, information subject, type of personal information, retention period, recipient scope, description of security measures)	Detailed log of processing action	A detailed log of the processing action should be recorded and kept.
Security processing (§32①a)	pseudony-misation	In order to guarantee anonymity, it is necessary to provide functions such as masking as a pseudonymisation measure for the video.
Security processing (§32①a, b)	Encryption / confidentiality	Encryption shall be applied to the stored videos to prevent private use and leakage by the controller and the processor. It also requires the same functionality where transferring to a third party.
Security processing (§32①b) Personal information security technical measures (§5①f) 6)	Integrity	It shall take steps to ensure the integrity of video storage and transfer to third parties.
Security processing (§32①c)	Stability in case of an accident	It is necessary to rigorously systematize management of relocation (export) to a

		third party along with detailed log recording and archiving of the processing action so that it can be traced in case of privacy invasion and outflow such as non-use of image.
Security processing (§32④)	Unauthorized processing restrictions	It shall provide detailed log management for process and non-jurisdiction access control.
Notice of Violation (§33)	Abuse and misuse audit	It is necessary to provide a tracking function that can instantly confirm illegal violations of videos and perform audits, and to generate and transmit a transparency report of the processing behavior in a systemized
Right to access personal information (§15①) 8)	View of video subject	It shall provide legitimate personal information by the subject of information, that is, the right of viewing of the video, and provide the non-discrimination function by the anonymity mosaic to the third person in addition to the information subject.
By design and by default data protection measures (§25) 4)	Processing history and audit function	For data protection measures for video processing equipment, Should be provided in the production of the product that is production of detailed processing records in the video information processing device and transmission to the external audit server and generation of electronic fingerprint (hash value) for providing integrity of the stored video.
Audit by controller (§28.3h)	Transfer operational log	Detailed processing records shall be generated, transmitted and maintained for the proper audit of the controller and the DPO on the processing behavior of the processor.
Legal / Process / Transparent Personal Information Processing (§5①a)	Audit management, Video supply management	Provide systemized functions for audit and third party transfer of Controller and DPO.
Justification of process (§6) 5)	Check processing purpose	It should generate, transmit, store, and provide periodic or non-periodic auditing of process action records to ensure fairness of process actions.
Personal information security technical measures (§5①f) 6)	Control of access rights	The access control function should be provided to the video.
Collection date and time accuracy	Standard Time Interworking	In order to precisely manage the process action, accurate time through standard time interlocking should be provided.
Move information to third parties	Delete / export video	It is necessary to ensure the integrity of the exported video by providing the basis of the export and providing the electronic fingerprint to guarantee the correspondence between the export and the original video.
Notification of safeguards in transit outside the EU (§15②)	Track video export	It provides the function of exporting the video through the system, and it should provide the function of notifying the right holder such as the video subject, the processor, the controller and the DPO(Data Protection Officer).
Right to be forgotten (§17①) 9)	Automatic deletion of personal information	It should support automated video deletion or anonymization by reasons such as disappearance of processing purpose, end of storage period, invasion of privacy etc.
Right to be forgotten (§17②) 10)	Obligation of video export notice	It should provide unified and systematic function for video export, prevent illegal export, manage legitimate export record, and inform the subject of information transfer.
Principle of processing personal information - Minimizing information (§5①C) 11)	Allow limited voice recording	In the case of video, the voice recording function should be originally limited, and the setting change behavior of the video information processing device should be recorded so that the related function can be used or not.

Ⅳ. Analysis of response technology for video information processing device

1. Response technology

앞서 제안한바와 같이 GDPR에서 영상에 요구되는 대응 기술은 VPIC로 대표하는 영상관리 절차 전반의 처리행위 내부통제, 표준시간 동기화와 무결성 그리고 제3자로의 이전 등 포렌식에 의한 처리 및 반출, 사생활 보호를 위한 투명성 보증 감사 등으로 나뉜다. 세 가지를 분석하여 제시하면 다음과 같다.

① 내부통제(Internal Control)

유출 등 사고 발생 시 원상회복은 거의 불가능하기 때문에 처리 행위를 실시간 모니터링 하여 즉각적 경고 및 조치가 이루어져야 한다. 해킹과 같은 외부자에 의한 악의적인 개인정보의 위변조, 삭제, 탈취에 의한 유출과 함께 처리자와 같이 합법적인 내부자에 의한 행위에 의한 사고는 GDPR에서 규정한 중대한 위반 사례가 되고 그 처벌을 중하게 하고 있다.

기존 개인정보지침(Directive)과 달리 GDPR은 명시적 규정이 없어 불가항력적으로 면책이 되거나 할 수 없기 때문에 내부통제는 최우선적으로 이루어져야 하고, 그를 위해서는 처리자의 처리 행위에 대하여 상세로그를 생성하여 영상정보의 유출 및 오남용 행위 이력을 즉각적으로 분석하고 통계데이터를 토대로 투명성 보고서를 작성하여 주기적인 감사가 이루어져야 한다.

통제자 또는 개인정보책임관(DPO)은 자신의 책임이 없음을 입증할 경우 면책도 가능하다는 것도 내부통제 기술이 반드시 필요한 이유라고 하겠다.

② 포렌식에 의한 처리 및 반출(Forensics)

모든 처리 행위에 대한 감사 및 추적을 위해서는 디지털정보에 대한 포렌식 기반 절차가 필요하고, 포렌식의 핵심은 표준시간과의 동기화를 통한 처리 행위 시각의 정확성과 원본 로그 보존처리에 의한 근거유지, 전자지문(해시값)에 의한 원본의 위변조 여부 입증이다.

포렌식 절차에 의하지 않은 처리 행위 기록의 생성, 보관은 무의미할 뿐 아니라 오히려 감사 행위를 방해하는 요소가 된다. 제3자에게의 이전 등과 같은 영상의 반출은 원본영상의 위변조의 이상 유무 확인 후 반출 절차를 진행하여야 유의미한 반출 행위와 결과를 값을 보증 받을 수 있고, 반출 절차를 시스템화함으로써 추후 발생할 수 있는 위변조 등 무결성의 시비를 원천적으로 차단 할 수 있다.

영상은 처리의 본래 목적에 항상 방범 즉 형사상 민사상 법적 증거자료로써 사용되기 때문에 법정에서 요구되어지는 엄격한 증거능력을 유지하여야 하고 이때 필요한 것이 포렌식 기법이다.

③ 사생활 보호(Privacy)

개인정보 즉 영상을 법에서 정의하고 규제를 하는 이유는 영상은 시각적 정보이고 민감한 개인적 사생활을 포함하고 있어 목적과 다르게 오남용 되거나 유출될 경우 정보주체자에게는 큰 피해가 발생하고, 처리자 및 그 소속 기관은 민형사상의 제재를 받기 때문이다.

CCTV 장비들에 의한 사생활 침해를 방지하기 위해서는 촬영, 전송, 보관과 운영하는 모든 장비에서 처리 행위 전반에 걸쳐 상세하고 명확한 기록을 남겨야 하고, 위변조 되지 않도록 보관하여야 한다. 또한 CCTV 촬영장치 중 PTZ(Pan Tilt Zoom)가 가능한 장치는 처리자에 의하여 촬영 목적에 벗어난 지역을 촬영하는 부정 수집행위에 대한 감시를 위해 PTZ행위의 기록과 PTZ행위 발생시 촬영 영상의 이미지 로그를 생성하여 관리를 하는 것이 필요하다.

2. Privacy by design

GDPR의 Privacy by design은 전체 공정에 걸쳐 privacy를 고려한 시스템 공학의 접근이다. 이 개념은 가치중시디자인의 즉 전체 과정에 잘 정의된 방법으로 인간가치를 고려한 한 사례이며, 그리고 이 가치중시디자인으로부터 유래되었다.

기본 7원칙은 다음에 기초하고 있다.

1.Proactive not reactive; Preventative not remedial
: 대응보다는 사전 예방, 치유가 아닌 예방
2.Privacy as the default setting
: 기본설정에 의한 Privacy
3.Privacy embedded into design
: 설계시에 Privacy 내재화
4.Full functionality – positive-sum, not zero-sum
: 완전한 기능, 제로섬이 아닌 양적 합
5.End-to-end security – full lifecycle protection
: 종단간 보안, 전체 생애주기 보호
6.Visibility and transparency – keep it open
: 가시성 및 투명성, 공개 유지
7.Respect for user privacy – keep it user-centric
: 사용자 Privacy의 존중, 사용자 중심 유지

위 7 원칙에 의한 자료보호는 EU내 자료보호를 단일 법률로 통일하려는 EU집행위원회 계획에 포함되어 GDPR로 제정되었다[9].

그러나 최신의 법도 protection by design이나 privacy by design을 정의하거나 인용문헌을 제시하지 않아 이 개념으로 무엇을 의미하는지 불분명한 점이 문제점이다. 이러한 점을 해결하려는 것이 VP(Video Privacy) SNMP-MIB 기술이다.

3. VP SNMP-MIB

IANA(http://pen.iana.org)에 PEN 42937로 등록된 VP SNMP-MIB은 SNMP Trap Notification Type으로 영상정보처리기기에서 내부통제서버로 전송되어지는 로그의 종류를 확인 할 수 있다[10].

VP SNMP-MIB에서는 NVS(Network Video Storage), NVT(Network Video Transmitter) 장치에 대한 상세로그를 Table 2, Table 3과 같이 정의함으로써 protection by design이나 privacy of design 개념을 명확하게 제시하였다.

Table 2의 NVS 로그 상세를 보면 크게 Access Log, System Log로 나뉘며, Access Log는 사용자 로그인 관련 행위, CCTV PTZ 제어행위, 실시간 뷰, 저장영상 검색 및 백업 행위를 정의하고 있고, System Log는 시스템 부팅과 공장초기화 행위, 사용자 및 그룹 설정 행위, 시스템에 의한 자동 PTZ 제어, 시스템 설정변경, 장애나 영상분석 등과 같은 이벤트 내역 마지막으로 저장영상에 대한 해시 값 생성 행위를 정의하고 있다.

Table 3의 NVT 로그 상세를 보면 크게 NVS와 같이 크게 Access Log, System Log로 나뉘며, Access Log는 사용자 로그인 관련 행위, CCTV PTZ 제어행위, 실시간 뷰, 저장영상 검색 및 재생 행위를 정의 하고 있고, System Log는 시스템 부팅과 공장초기화 행위, 사용자 및 그룹 설정 행위, 시스템에 의한 자동 PTZ 제어, 시스템 설정변경, 장애나 영상분석 등 이벤트 행위를 정의하고 있고, 두 표의 큰 차이는 NVS는 저장장치이고, NVT는 촬영 및 전송을 주목적으로 하고 있어, 저장영상에 대한 해시값 생성과 백업 행위에 대한 처리가 NVT에는 없다는 점이다.

Table 2. NVS Log Specification

Log type	Object	Specification	Description
Access Log	Other	Reserved	Reserved
	User	User Log In	User logins successful
		User Log Out	User Logouts succesful
		User LogIn Fail	User logins faile
		User LogIn Lock	Locks on failure over specified number of logins
		User LogIn Block/Deny	User connects with blocked IP or user account
	PTZ Control	Manual Start(Move)	User start(Move)s control of PTZ or Focus
		Manual Stop	User stops control of PTZ or Focus
	Live View	Start	User starts watch live video or events
		Stop	User stops watch live video or events
	Video Playback (Search)	Start	User start playback or search saved video
		Stop	User stop placyback or search saved video
		Control (Play, FF, Rew 등)	User cotrol play, FF, REW etc. saved video
	Video Backup	Start	User start backup saved video
		Stop	User stop backup saved video
		Hash	Generate secondary hash value for integrity verification when backing up video
System Log	Other	System Boot	Boot system
		System Shutdown	Shutdown system
		System Reboot	Reboot system
		System Factory Reset	Reset factory of system
		System Upgrade	Upgrade System firmware and software
	User	Add User	Add user
		Delete User	Delete user
		Modifiy User	Modify user
		Add User Group	Add user group
		Delete User Group	Delete user group
		Modifiy User Group	Modify user group
	PTZ Control	Move Start	System starts PTZ control
		Move Stop	System stops PTZ control
		Touring	System control PTZ by touring setting
		Presest	System control PTZ by presetting
	Configuration	Other	Change System Settings (Other Settings)
		Video	Change system video or audio settings
		Network	Change system network-relate settings
		Event	Change system event-related settings
		Time	Change time-related settings such as system NTP
		Storage	Change storage-related settings on your system
		Hash	Change hash settings for integrity verification
	Event	Other	Occur other event
		Trouble	Occur fault event
		Sensor	Occur sensor (input, output) event
		Relay	Occur relay event
		Motion Detection	Occur motion detection event
		Video Analytics	Occur event by video analytics
		Heart Beat	Transmit heart beat periodically
		Time	Change time period by NTP interworking
		Hash	Occur forgery or modulation saved videos
		Record	Start or end recording
	Hash/Forensics	Other	Occur other event
		Create	Create a hash information for the saved video file
		Delete	Delete a hash information for the saved video file

Table 3. NVT Log Specification

Log type	Object	Specification	Description
Access Log	Other	Reserved	Reserved
	User	User Log In	User logins successful
		User Log Out	User Logouts succesful
		User LogIn Fail	User logins faile
		User LogIn Lock	Locks on failure over specified number of logins
		User LogIn Block/Deny	User connects with blocked IP or user account
	PTZ Control	Manual Start(Move)	User start(Move)s control of PTZ or Focus
		Manual Stop	User stops control of PTZ or Focus
	Live View	Start	User starts watch live video or events
		Stop	User stops watch live video or events
	Storage	Search	User search saved videos
		Download	User backup saved videos
		Remove	User remove or Eject storage device
		Format	User fomat Storage device
		Play	User start playback saved video
		Stop	User stop placyback saved video
System Log	Other	System Boot	Boot system
		System Shutdown	Shutdown system
		System Reboot	Reboot System
		System Factory Reset	Reset factory of system
		System Upgrade	Upgrade System firmware and software
	User	Add User	Add user
		Delete User	Delete user
		Modifiy User	Modify user
		Add User Group	Add user group
		Delete User Group	Delete user group
		Modifiy User Group	Modify user group
	PTZ Control	Move Start	System starts PTZ control
		Move Stop	System stops PTZ control
		Touring	System control PTZ by touring setting
		Presest	System control PTZ by presetting
	Configuration	Other	Change System Settings (Other Settings)
		Video	Change system video or audio settings
		Network	Change system network-relate settings
		Event	Change system event-related settings
		Time	Change time-related settings such as system NTP
		Storage	Change storage-related settings on your system
		Hash	Change hash settings for integrity verification
	Event	Other	Occur other event
		Trouble	Occur fault event
		Sensor	Occur sensor (input, output) event
		Relay	Occur relay event
		Motion Detection	Occur motion detection event
		Video Analytics	Occur event by video analytics
		Heart Beat	Transmit heart beat periodically
		Time	Change time period by NTP interworking
		Hash	Occur forgery or modulation saved videos
		Record	Start or end recording

4. VPIC(Video Privacy Internal Control)

본 논문에서 GDPR과 국내 개인정보보호법의 규정과 함께 관련 VP 기술, 원칙 등을 토대로 영상정보에 대한 내부통제 즉 VPIC에서 요구되는 기능별 분류한 결과, 디지털 포렌식, 감사관리, 운영관리, 영상제공관리의 큰 범주의 기능요소로 구분하여 4가지로 제시할 수 있다. 이것을 Table 4. Table 4에 요약 하면 다음과 같다.

표에서 첫째, 디지털 포렌식(digital forensics)은 내부 저장영상의 무결성 검증, 내부 영상 저장시 암호화, 시간동기화, 해시정보 활용기능이 있다. 내부저장영상에 대하여 무결성을 검증하기 위해 해시정보를 생성하여 위변조 검증시 비교해시정보로 활용하고, 비교해시정보의 신뢰도를 향상시키기 위해 제3의 서버로 해시정보를 전송함과 동시에 공개게재와 같은 외부공표 과정이 필요하다.

둘째, 감사관리(audit management)는 운영(행위)로그 수집 및 관리기능, 실시간 영상 오남용 감사기능, 영상정보 부정수집 통제, 장비 접속 차단/허용 기능, 사용자 계정별 권한 관리, 투명성 보고서로 나눌 수 있다. 인가된 사용자에 의해 영상정보처리기기 처리

행위를 실시간으로 로그를 수집하여 업무목적외 임의 사용행위, 목적외 정보 수집행위, 비권한 내지 초과권한의 접속 행위, 계정 권한 설정 변경 행위를 토대로 이력 등 통계자료를 기반으로 영상정보처리기기 운영에 대한 투명성 보고서의 생성 관리가 필요하다.

셋째, 운영관리(operation management)는 장비관리, 장애현황 및 장비 이벤트 관리로 구분된다. 24시간 가용성 확보를 위해 운영하는 장비의 체계화된 관리가 필요한데, 이를 위해서 장비의 설치, 변경, 교체 등의 이력과 장애 조치 내용, 장비 이벤트 현황을 관리하여야 한다.

넷째, 영상제공관리(video supply management)는 영상제공, 영상관리 내역, 영상 마스킹으로 나눌 수 있다. 영상제공 기능의 관리와 제공된 영상의 추적 관리, 그리고 제공영상에 대한 제3자 정보를 비식별화하는 마스킹 기능이 필요하다.

Table 4. VPIC Classification of Specification Function

Classification	Function	Specification
Digital Forensics	Verification of stored video integrity	Generate hashes for integrity verification of stored video
		Forgery inspection and events on stored video
		View hash creation, deletion historys for integrity verification
	Encryption for video storage	Encryption function for stored video
	Time synchronization	Interworking with standard time
		Automatic equipment time synchronization
	Hash information utilization function (hash bank)	Confirmation of video recording using hash information
		Video verification (reverse verification) and certificate issuance
Audit Management	Collection and Management operational (activity) logs	Create and view various operational logs
		Provide external audit through operational log transfer
		Provide original log analysis tool
		Generate information for collection log integrity verification
		Provides collection log forgery test
		Provides collected log duplication management
	Real-time video abuse audit function	Providing events for off-hours access
		Provide events for factory reset
		Provide event for user login failure or user account lockout
		Provide firmware upgrade event
		Providing events when adding or changing user accounts
		Providing event when blocked or allowed IP connection
		Generate Event Image Log
		Event extraction function by user rule
		Provide event pop-ups
		Provide push notifications
		Providing SMS for event alarm
	Video information illegal collection control function	Provide event when PTZ control range is exceeded
		Generate Image Log when controlling PTZ
	Block or allow access to equipment	Device access blocking function
		Allow access to equipment
	Manage permissions by user account	Authorization granularity per user account
		Auditor privileges for saved video backup
	Transparency Report	Remote connection status
		Video backup history
		Video search history
		Abuse Misuse history
		Trouble history
		Video Supply history
		Configuration change history

Ⅴ. Conclusion

본 논문에서는 곧 시행될 GDPR의 규정조항과 개인정보보호법과를 비교하여 대응기술에 대해 연구하였다. 우리나라에서 2011년부터 시행된 개인정보보호법은 GDPR에서 규정한 규제들을 이미 대부분 적용하고 있음에도 불구하고 국내에서 판매되는 국내외를 대부분의 CCTV 제품들이 관련 규정을 충족하기에는 일부 제품들을 제외하고는 일부제품을 제외한 대부분의 CCTV 제품들이 관련 규정을 충족하기에는 미흡하다. 이는 강력한 규제가 있음에도, 제대로 된 내부통제시스템의 정의의 부재와 관련 부처의 느슨한 감독 및 명확한 관련 지침이 없기 때문이다.

사실 우리나라는 국회에 개인영상정보보호포럼 등 민간 비영리 단체들이 영상정보의 특성에 맞게 오남용과 유출 방지, 그리고 형사소송법상 증거능력 확보를 위하여, 포렌식에 기반 한 내부통제기술에 대하여 관련 기술의 발굴과 표준화 및 미비 법규 개정 등을 추진해 왔고, 어느 정도 관련 기술이 정착화 되고 있어 손쉽게 우리나라 개인정보보호법과 GDPR의 규제를 충족시킬 수 있다.

현재 전 세계적으로 개인정보 규제를 강화하려고 하며, 그 흐름을 유럽연합이 주도하고 있다. GDPR이 적용되는 2018년부터 유럽은 우리나라와는 다른 분위기가 형성될 것으로 보이며, EU 회원국의 합의에 의한 규정이 제정되기까지 오랜 시간이 걸렸지만, 제정되고 시행되게 되면 규정과 매뉴얼에 의해 엄격한 준수를 요구하고, 위반 시 규정에 의한 강력한 제재가 이루어질 것으로 보인다. 따라서 우리나라도 이에 대한 대응기술 마련이 필요하다.

향후 연구에서는 privacy by design의 7원칙에 대하여 영상정보 수집부터 파기까지의 전처리과정에 대한 설계 및 구현에 대하여 좀 더 깊이 있게 연구하고자 한다.

REFERENCES

[1] Ki-Il Ryu, “CCTV Observer? Protector?", Personal Video Information Protection Forum, 3rd Regular Seminar, 2014

[2] Young-im Cho, "Personal Information Protection and Intelligent Agent Technology", Journal of the Korean Institute of Information Scientists and Engineers, Vol.6, No.1, pp.29-35, Dec. 2008

[3] Ki-Il Ryu, "Expert Interview of Personal Information Protection Act", Security World a Monthly Magazine Sep. 2013

[4] Korea National Information Society Agency, "Integrated Control Center Construction Guideline (Procedures for Establishment of Integrated Control Center,

Standard Model for Integrated Control Center)", Korea National Information Society Agency, 2011
[5] The EU Parliament and of the Council, “General Data Protection Regulation”, Official Journal of the European Union, 4.5.2016, 27 April, 2016
[6] Il-hwan Kim, "GDPR Supervision Organization", Institute for Information Human Rights, GDPR Lecture, 2016
[7] Sang-Min Kim, "Amendment of Personal Information Protection Act", Korea 19th National Assemblyman, 2013
[8] Weon-Kook Kim, "Internal Control Technology Trends for Personal Video information Protection", 4Dream Co., Ltd., VIDEO PRIVACY SOLUTION DAY, 2014
[9] https://en.wikipedia.org/wiki/Privacy_by_design, 2017
[10] Ki-Il Ryu, "VPM Technology Trend and Standardization Direction," 4Dream Co., Ltd., VIDEO PRIVACY SOLUTION DAY, 2014

Authors

Ki Il Ryu received his B.S. degree in Computer Science from Kangwon National University in 1999, his M.S. degree in Information Security from Chonnam National University in 2011 and now is a Ph.D. course student in computer engineering from Gachon University.
He worked as a cyber criminal investigator at the National Police Agency until 2010. He interests personal video information protection, forensics, and artificial intelligence.

Young Im Cho received her B.S., M.S., and Ph.D from the Department of Computer Science, Korea University, Korea, in 1998, 1990 and 1994, res, respectively She is a professor at Gachon University. Her research interest include AI, big data, information retrieval system, smart city, cloud etc.