영상정보처리기기(CCTV)의 포괄적 보안관리를 위한 암호·인증·보호·체계(CCPS) 모델 제안

송원석[1,*] · 조준하[1] · 강성문[1] · 이민우[2]

[1]안보지원사령부 국방보안연구소 · [2]아주대학교

Proposed CCPS model for comprehensive security management of CCTV

Won-Seok Song[1,*] · Jun-Ha Cho[1] · Seong-Moon Kang[1] · MinWoo Lee[2]

[1]Defense Security Support Command · [2]Ajou University

E-mail : s506439@dssc.mil.kr / wearegoodman@naver.com / smkang111@korea.com / iminu@ajou.ac.kr

요 약

영상정보처리기기(CCTV)는 민감 정보를 수집, 전송, 저장하는 데 있어서 관리적, 물리적, 기술적 측면에서 포괄적으로 보안관리가 이뤄져야 한다. 이를 위해 영상정보처리에 관련된 암호기술, 기술인증, 보호기술, 보안장비에 대한 적용 기준이 필요하다. 본 논문에서는 영상정보처리기기에 관련된 다양한 보안기술, 인증제도를 분석하여 영상정보처리기기의 구축 및 운영에 적용하여 포괄적 보안관리를 위한 암호·인증·보호·체계(CCPS; Cryptography·Certification·Protection·System) 모델을 제안한다.

ABSTRACT

A video information processing system (CCTV) requires comprehensive administrative, physical, and technical security management to collect, transmit and store sensitive information. However, there are no regulations related to video information processing, certification methods for the technology used, and application standards suitable for security technology. In this paper, we propose a cryptography, certification, protection, system (CCPS) model that can protect the system by including encryption technology for application to the video information processing system and authentication measures for the technology used in the system configuration.

키워드

Intelligent CCTV, Security Model, Surveillance, Privacy

Ⅰ. 서 론

영상정보처리기기는 일상생활의 사회안전 분야, 군사 작전의 감시, 정찰 분야에 이르기까지 폭넓게 사용되고 있다. 또한 인공지능과 빅데이터 기술을 적용하여 성능과 기능이 확장된 지능형 영상정보처리기기는 민감 데이터를 생성하고, 전달하며, 저장하는 용도로 사용되고 있다.

이에 반해 영상정보처리기기가 지능화됨에 따라 네트워크에 의한 위협이 다양해지고, 민감 정보 노출에 따른 피해 규모와 영향력은 많이 증가하고 있다.

이 때문에 지능형 영상정보처리기기에 대한 보안관리는 매우 중요하다. 영상정보처리기기를 안전하게 운영하기 위해서는 장비의 개발, 설치, 운영에 대한 전체 생명주기를 대상으로 포괄적인 보안관리가 이뤄져야 한다. 영상정보처리기기에 대한 암호기술, 기술인증, 보호기술, 보안장비가 다양하고, 시스템 구현이 복잡하기 때문에 적절한 포괄적 보안관리 방안을 마련하는 것이 필요하다.

본 논문의 구성은 다음과 같다. 2장에서 영상정보처리기기의 데이터 분류(안)과 3장에서 데이터처리 단계별 포괄적 보안관리 방안인 CCPS를 살펴본다. 4장에서는 데이터 상태를 “생성, 전송, 저장, 열람/반출” 단계로 구분하고 CCPS의 적용방안 예를 제시하고, 5장에서 결론을 맺는다.

* speaker

II. 영상 데이터 분류(안)

국방 무기체계 분야에서 활용하고 있는 위험관리프레임워크(RMF, Risk Management Framework)의 제1단계는 보호 대상인 자산을 식별하는 것이다. 영상정보처리기기에 대한 보안관리 역시 보호 대상인 영상 데이터를 식별하는 것부터 우선적으로 수행되어야 한다.

따라서 비용 대비 효과성을 고려하여 영상 데이터를 구분하여 보안관리를 적용하기 위해서는 <표 1>과 같이 영상 데이터를 분류하는 것이 필요하다.

표 1. 영상 데이터 분류(안) 예시

구분	예시
비밀 (비공개)	경계작전용: GOP, 해안초소, 중요시설, 함정 등 무기체계로 도입되는 영상정보처리기기에서 생성, 전송, 저장, 열람/반출이 이뤄지는 영상 데이터
일반 (공개)	부대관리용: 탄약창고, 비행장 등 전력지원체계 사업으로 도입되는 영상정보처리기기에서 생성, 전송, 저장, 열람/반출이 이뤄지는 영상 데이터

영상 데이터는 조직 내부에서 접근 권한이 부여된 제한된 인원에게만 공개하는 '비밀' 데이터와 그 외 필요시 공개가 가능한 '일반' 데이터로 분류할 수 있다. 예를 들어 군사 보안과 관련된 상황에서 '경계작전용'은 비밀 데이터로 분류하고, 일반적인 '부대관리용'에서 사용되는 영상 데이터는 일반 데이터로 분류하는 것이 적합하다.[1, 2]

III. 영상정보처리기기 포괄적 보안관리 모델

본 연구에서는 지능형 영상정보처리기기의 데이터 분류(안)을 제시하고 각 데이터의 상태를 기준으로 <표 2>와 같이 "생성, 전송, 저장, 열람/반출"로 데이터 처리 단계별 보안관리 방안을 살펴본다.

표 2. 영상정보처리기기 데이터 처리 단계

구분	데이터 상태
생성	영상 데이터가 수집되는 상태 비정형 데이터로서 저장, 전송 준비
전송	영상 데이터가 전송되는 상태 유/무선 통신 방식에 따라 구분
저장	영상 데이터가 저장되는 상태 저장 방식에 따라 구분
열람/반출	영상 데이터를 활용하는 상태 재생, 분석에 활용

표 3. 포괄적 보안관리 모델 (CCPS)

구분	요구기술
암호기술 (Crypto-graphy)	CR1: 국가용 암호장비 CR2: 영상 암호기술 CR3: 양자 암호기술 CR4: 무선 암호기술
기술인증 (Certifi-cation)	CE1: 지능형CCTV성능시험(KISA) CE2: CCTV 장비 보안인증(TTA) CE3: 공통평가기준(CC, KISA) CE4: 암호모듈검증(KCMVP, KISA/NSR) CE5: 데이터보안인증(KDATA)
보호기술 (Protec-tion)	PR1: ZTS PR2: SDN PR3: DB암호화 PR4: 영상 자동 마스킹 PR5: 교차영역솔루션
보안장비 (System)	SY1: WIPS/IPS SY2: F/W SY3: EDR SY4: Anti-Virus SY5: DLP/DRM

본 연구에서는 지능형 영상정보처리기기에 대한 포괄적 보안관리 모델을 <표 3>과 같이 암호기술, 기술인증, 보호기술, 보안장비로 구현하였다.

암호기술은 보안목표를 달성하기 위해 안전성이 검증된 것을 사용하도록 한다. CR1은 비공개 영상 데이터 전송시 국가용 암호장비를 사용하는 경우이다. CR2는 영상 데이터의 실시간 인코딩(encoding)이 필요한 경우이다. CR3는 양자기술을 이용한 암호키 분배가 필요한 경우이다. CR4는 영상 데이터의 무선 전송이 필요한 경우이다.

기술인증은 지능형 영상정보처리기기의 개발, 구축, 운영에 필요한 국내 인증제도를 사용하도록 한다. CE1은 한국인터넷진흥원(KISA)에서 주관하며 지능형 CCTV 성능시험 인증으로 이벤트별로 세부 시험 조건을 제시하여 성능을 인증할 수 있다.[3] CE2는 한국정보통신기술협회(TTA)에서 주관하며 CCTV 장비의 성능에 대한 시험을 수행하므로 영상정보처리기기의 장비에 대한 품질 검증과 그 결과를 인증할 수 있다.[4] CE3는 KISA에서 주관하며 기존 공공기관에 도입되는 보안장비에 대한 공통평가기준으로서 인증장비 확인에 적용된다.[5] CE4는 한국형 암호모듈검증제도 (KCMVP; Korea Cryptographic Module Validation Program)로서 안전한 암호기술의 적합한 사용을 인증한다.[6] CE5는 한국데이터산업진흥원(KDATA) 주관하며 데이터 보안에 대한 기술요소 전반을 심사하여 인증한다.[7]

보호기술은 지능형 영상정보처리기기의 전사적 운영에 있어서 필요한 기술을 사용하도록 한다. PR1은 ZTS (Zero Trust Security)로서 적절한 인증절차 없이는 그 어떤 접근도 허용하지 않는

것을 목표로 한다. PR2는 SDN (Software Defined Network)로서 가상화 기반체계에서 구현되는 네트워크 환경에 대한 보안관리가 필요함을 의미한다. PR3는 데이터베이스 암호화로서 보호의 대상이 되는 데이터의 암호화를 의미한다. 이로써 민감 데이터를 보호하고 데이터 탈취, 비인가 접근으로부터 데이터 기밀성과 무결성을 보장한다. PR4는 지능형 영상정보처리기기에서 카메라로부터 수집된 영상 데이터, 또는 이미 저장된 영상 데이터에서 민감 정보를 마스킹하는 기술을 적용한다. PR5는 일방향 전송기술을 이용하여 물리적, 전기적, 논리적으로 상이한 네트워크 도메인으로 구분하는 보안기술이다.

보안장비는 심층방어 (defense in depth)의 개념에서 지능형 영상정보처리기기를 구축하는데 필요한 보안장비들을 제시한다. SY1은 무선과 유선 네트워크 환경에서 침입탐지시스템 (IPS; Intrusion Prevention System)을 구축함으로써 알려진 위협을 탐지하고 공격을 차단한다. SY2는 방화벽 (firewall)을 구축함으로서 패턴기반과 행위기반으로 위협을 탐지하도록 한다. SY3는 EDR (Endpoint Detection & Response)로서 호스트와 단말에서 탐지와 대응 능력을 갖추도록 하는 것이다. SY4는 시스템 관리와 운영에 사용되는 호스트 응용체계에서 악성코드를 탐지하기 위한 것이다. 끝으로 SY5는 민감 데이터의 유출을 예방하고 유출되더라도 사용될 수 없도록 DLP (Data Loss Prevention)와 DRM (Digital Right Management)을 구현하는 것이다.

Ⅳ. 포괄적 보안관리 CCPS 모델 적용 예시

본 장에서는 앞서 제시된 영상 데이터 분류(안)과 영상정보처리기기 포괄적 보안관리를 위한 CCPS 모델 적용 예를 제시한다.

표 4. 비공개 영상 데이터의 포괄적 보안관리

구분		데이터 상태			
		생성	전송	저장	열람/반출
비공개	C	CR1 CR2	CR1 CR3 CR4	CR1 CR2	CR2
	C	CE1 CE3 CE4 CE5	CE3 CE5	CE2 CE3 CE4	CE3 CE4 CE5
	P	PR1		PR3 PR4	PR4
	S	SY3	SY5	SY2 SY3	SY2 SY4
				SY4 SY5	SY5

먼저 <표 4>는 군의 경계작전에 사용되는 영상 데이터를 비공개로 분류하는 경우이다. 데이터 상태에 따라 보안관리를 암호기술, 기술인증, 보호기술, 보안장비 순으로 CCPS 모델의 요구기술을 선정하였다. 각 요구기술들은 미래 신기술 개발을 고려하여 탄력적으로 적용할 수 있도록 지속적인 관리가 필요하다.

<표 5>는 군의 부대관리, 사회안전 분야와 같이 일반적으로 영상 데이터를 공개로 분류하는 경우이다. 공개 영상 데이터에 대해서도 현재 관련 규정에서 요구하는 보안목표와 이를 달성하기 위한 적정 기술 수준에 맞춰 가시적으로 포괄적 보안관리를 적용하는 데 활용될 수 있음을 볼 수 있다.

표 5. 공개 영상 데이터의 포괄적 보안관리

구분		데이터 상태			
		생성	전송	저장	열람/반출
공개	C	CR2	CR2 CR3 CR4	CR2	CR2
	C	CE2 CE3 CE4 CE5	CE3 CE4	CE1 CE3 CE4	CE4
	P		PR2 PR5	PR3 PR4	PR4
	S		SY1 SY3 SY5	SY4 SY5	SY4 SY5

Ⅴ. 결 론

본 논문에서는 지능형 영상정보처리기기에 대한 포괄적 보안관리를 위해 영상 데이터 분류, 데이터 상태별 암호기술, 기술인증, 보호기술, 보안장비를 적용하는 CCPS 모델을 제시하였다.

4차산업혁명 및 5G 통신 기술의 발전으로 인해 영상 데이터 활용이 증가하고, 다양한 위협에 직면하면서 포괄적 보안관리는 중요해졌다. 본 연구결과는 군의 신규 영상정보처리기기 도입 및 구축 사업시 적용할 수 있으며, 향후 영상 데이터 보안 강화를 위한 정책 자료로 활용이 가능하다.

References

[1] Directive on *Defense Security Operations CCTV Security Management,* Article 146-2, ROK.

[2] Directive on *Defense Privacy,* Section 5, ROK.
[3] Intelligent testing and certification plan for defense projects, 2017, KISA.
[4] Security Performance of IP Cameras for Public Institutions, 2020, TTA.
[5] Common Criteria (http://www.itscc.kr/)
[6] KCMVP (http://www.nis.go.kr/)
[7] KDATA (http://www.dqc.or.kr/)