Journal of the Korea Convergence Society
Vol. 8. No. 11, pp. 93-101, 2017
https://doi.org/10.15207/JKCS.2017.8.11.093

인원 출입 권한과 연계한 스마트폰 카메라 제어 시스템

전병진[1], 한군희[2], 신승수[1*]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부

Smartphone Camera Control System in connection with Personnel Access Rights

Byung-Jin Jeon[1], Kun-Hee Han[2], Seung-Soo Shin[1*]
[1]Department of Information Security, Tongmyong University
[2]Division of Information & Communication Engineering, Baekseok University

요 약 본 연구의 목적은 기업체의 임직원이나 협력사 직원들이 스마트폰 카메라를 이용해 기업의 제품 도면이나 기밀유지가 보장되어야 하는 제품 개발 시 진행되었던 업무 내용이 저장된 문서 등을 스마트폰 카메라로 촬영하여 외부로 유출하는 것을 사전에 차단하고자 한다. 본 연구에서는 허가된 사용자에 대한 사진 촬영과 기업체 내부에서만 촬영된 데이터를 공유할 수 있게 하는 인원 출입 권한과 연계한 스마트폰 카메라 제어시스템을 제안한다. 이를 위해 기업체에 상주하는 임직원, 협력사 직원들과 방문객들의 스마트폰 제어 프로그램(MCS : Mobile Camera Control System) 대한 설치현황을 개발하여 출입이 허가된 지역에서 설치된 스마트폰 제어 프로그램 작동여부를 실험 및 분석한다. 또한, 방문객들이 기업체 방문 시 스마트폰 카메라를 통한 사진 촬영의 방지효과와 스마트폰 카메라 렌즈부분에 부착하는 봉인 스티커 비용의 절감효과가 나타났다.

• **주제어** : 정보유출, 스마트폰제어, 인터페이스, 인원출입관리, 본인인증

Abstract The purpose of this paper is to investigate the effect of the smart phone camera on the company's employees or employees of partner companies, we want to block things in advance. In this paper, we propose a smart phone camera control system which is connected with the personnel access right which enables to share the photographed image of the authorized user and the data shot only within the enterprise. To this end, we have developed the installation status of smart phone control program (MCS: Mobile Camera Control System) of employees, employees and visitors of company, and experimented and analyzed whether the smart phone control program installed in the authorized area. In addition, when visitors visited the company, the effect of prevention of photograph shooting through smart phone camera and the cost of seal sticker attached to the smart phone camera lens part were reduced.

• **Key Words** : Information leakage, Smart phone control, Interface, Personnel access, Authentication

*Corresponding Author : 신승수(shinss@tu.ac.kr)
Received October 2, 2017
Revised November 6, 2017
Accepted November 20, 2017
Published November 28, 2017

1. 서론

ICT의 발전과 더불어 스마트폰 관리시스템이 나날이 발전하고 있다. 그에 따라서 모바일 기기 사용의 증가로 정보 수집 및 처리 등이 손쉽지만, 정보유출로 인한 기업 손실이 커지고 있는 상황이다[1]. 글로벌 산업 시대에서 기업이 보유한 자산정보(제품 도면 또는 생산 라인 현황 등)는 그 기업의 경쟁력을 확인할 수 있는 중요한 척도라고 할 수 있다[2]. 스마트폰의 분실, 도난에 따른 정보유출 방지를 위해 MDM(Mobile Device Management 기술을 활용하고 있다[3]. 특히, 모바일 기기 중 스마트폰 카메라를 이용하여 생성한 정보를 상호간에 쉽게 공유할 수 있다. 그러나 기업의 정보유출은 외부의 악의적인 사용자로부터 발생하는 것보다 기업 내부의 모바일용 오피스 프로그램을 이용하는 정보 유출이 증가하고 있다[4].

기업체 내・외부의 악의적인 사용자에 의한 정보유출 때문에 기업에서는 법정 분쟁 등에 따른 비용 발생, 이미지 추락, 기업의 존폐까지도 위협받을 수 있다[5]. 내・외부의 악의적인 사용자에 의한 정보유출을 막기 위해 기업체에서는 DRM(Digital Right Management)과 DLP(Data Loss Prevention)을 도입하여 지속적으로 운영하고 있다[6]. 그러나 기업체에서 운영하고 있는 정보유출 관리시스템은 개인 컴퓨터(PC, LAPTOP)에 설치되어 정보유출을 방지하지만 모바일 기기를 이용한 정보유출은 사전에 방지할 수 없다[7]. 인원 출입통제 시스템은 보안상의 이유로 정보보안 관리자의 출입인원에 대한 철저한 업무 분석으로 권한이 있는 인원만 출입이 가능하고 인증되지 않은 인원은 출입을 허용하지 않는 시스템이다[8].

최근에는 분실한 스마트폰을 이용한 정보유출을 방지하고자 연산기반 패스워드 기법을 사용하여 사용자를 인증하는 방법[9]과 정확한 사용자 인증이 필요하지 않는 경우에는 사용자에게 편리성을 제공하고자 인증 절차를 없애버리는 어플리케이션들도 있다[10]. 효과적인 유・무선 정보유출 관리시스템은 악의적인 사용자의 모바일 기기를 이용한 정보유출을 사전에 차단하고, 합법적인 사용자의 모바일 기기 사용으로 인한 업무 능률을 저하시키지 않는 두 가지 경우를 동시에 만족시킬 수 있어야 한다. 이러한 상황에 맞게 기업체의 정보를 효율적으로 관리할 수 있는 새로운 제어 시스템이 필요하다.

본 논문에서는 인원 출입 권한과 연계한 스마트폰 카메라 제어 시스템(SCPA : Smart phone camera Control system linked with Personnel Access right)을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 스마트폰 카메라를 이용한 정보유출에 관련된 연구를 분석하고, 3장에서는 인원 출입 권한과 연계한 스마트폰 카메라 제어 시스템에 대해 설명한다. 4장에서는 인원 출입 권한과 연계한 스마트폰 카메라 제어 시스템의 차단 효과를 분석하고 5장에서는 결론을 맺는다.

2. 관련 연구

최근에 스마트폰의 본인인증 방법과 본인인증의 보안성을 강화하면서 사용자의 편의성도 높일 수 있는 연구들이 진행되고 있다. 스마트폰 본인인증 방법은 연산자와 연산 값을 설정하여 잠금을 해제할 때 연산자와 입력한 수의 연산 결과 값이 일치하는지 확인하는 방식이다. 연산기반 패스워드 방법을 통해 본인 스마트폰이 아닌 경우는 일정 시간 잠그는 기능과 비인가 접근이 확인되는 경우 잠금 기능에 비인가자의 얼굴을 촬영하여 소유자가 비인가자를 확인할 수 있는 카메라 액션을 추가하는 방식을 용승림 등이 제안했다[11].

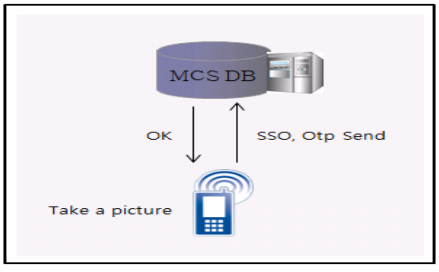
또한, 보안성과 사용자의 편의성을 높일 수 있도록 김지환 등[10]이 제안한 방법은 스마트폰의 센서를 이용하여 주변의 상황을 파악하고, 파악된 상황에 대한 타인의 접근가능 수준을 수치화하여 측정했다. 그리고 측정된 접근가능 수준을 합산하여 상황 위험도가 특정수준에 도달했을 때 인증을 요청한다. 인증 요청을 인지하기 위해 스마트폰을 이용해 상황을 추론하는 기능인 상황인지 계층과 위험도를 측정하고 누적시켜 누적위험도를 계산하는 단계인 상황위험도 계층과 인증요청을 판별한다.

기업체에서는 스마트폰의 빠른 보급으로 업무와 관련된 회의 내용이나 기업 내의 시설물에 대한 정보를 영상으로 촬영해서 정보를 공유한다. 이러한 무분별한 정보공유를 방지하고자 도입한 MCS(Mobile Camera Control System) 프로그램은 설치 후 사내 포털 서비스와 연동되어 한 번의 인증과정으로 한 디바이스 내의 여러 사이트에서 자원을 이용 가능하게 하는 인증 기능(SSO : Single Sign-On)[12]과 고정 비밀번호 대신 무작위로 생성한 비밀번호로 사용자를 인증하는 방법(OTP : One Time Password)[13,14,15]의 두 가지 인증방식이 실행된다. 두 가지 인증방식이 실행되면 기업 내의 모든 지역에서 사진 촬영이 가능하다. 따라서 기업체의 시스템 구성과 업

무 흐름에 대한 사례를 분석하여 스마트폰 카메라를 이용한 정보유출을 방지를 위한 시스템을 도입했다. 정보유출을 방지하기 위해서 임직원, 협력사 직원들과 방문객들은 사내 포털시스템에 접속해서 MCS 프로그램을 개인 스마트폰에 설치한다. 만약 MCS 프로그램을 삭제할 경우, IDCARD로 사무실 출입 시 경광등이 자동으로 작동하게 되면 해당 직원은 MCS 프로그램을 설치해야만 출입할 수 있다.

설치된 MCS 프로그램은 사내 출입 시 자동으로 작동되고, 사내를 벗어나면 자동으로 정지된다. MCS 프로그램이 작동이 되면 스마트폰에 내장되어 있는 카메라 기능은 작동되지 않고 LMCP(L's Mobile Camera Program)이 작동되어 스마트폰의 데이터 통신 기능을 차단하고 기업체의 Wi-Fi만 사용할 수 있다.

LMCP가 작동되면 Wi-Fi로 기업체의 정보유출 모니터링 시스템과 연결되어 실시간으로 촬영한 데이터를 확인할 수 있다. LMCP로 촬영한 데이터는 스마트폰의 hidden영역에 암호화된 상태로 저장되어 사내를 벗어나면 데이터를 확인할 수 없다. 여기서 스마트폰의 hidden 영역은 LMCP가 작동된 상태에서만 사용자에게 표시되는 메모리의 암호화된 영역이다. 이와 같이 스마트폰을 이용한 정보유출 방지 시스템은 [Fig. 1]과 같다.



[Fig. 1] MCS System

MCS 프로그램은 정보보안 관리자의 승인으로 설치되었기 때문에 사·내외 어디서든 작동이 되어도 문제가 없다. 하지만, MCS 프로그램 내의 LMCP는 정보보안 관리자가 승인한 출입 지역에서만 작동이 되어야 한다. 그래서 임직원, 협력사 직원과 방문객들의 MCS 프로그램 설치 현황 관리와 인원 출입권한과 연계한 스마트폰 카메라 제어 시스템을 제안한다.

본 논문에서 제안하는 SCPA 시스템의 목적은 기존의 스마트폰에 설치한 MCS 프로그램의 설치현황을 신속하게 파악하고 인원 출입 권한과의 정보연계를 통해 스마트폰 카메라를 통한 정보유출을 사전에 차단하는 것이다. 그리고 기업체를 방문하는 방문객들에게 정보유출 방지를 위해 스마트폰 카메라에 부착하는 봉인 스티커의 비용을 줄일 수 있다.

3. 인원 출입 권한과 연계한 스마트폰 카메라 제어 시스템

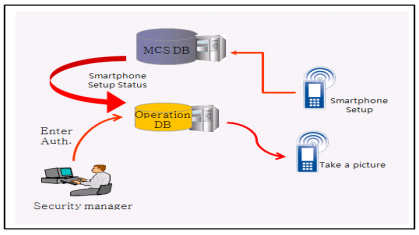
본 장에서는 임직원, 협력사 직원들과 방문객들이 스마트폰 카메라 촬영으로 기업 내의 정보를 유출할 수 있는 방법이 다양하게 존재하기 때문에, 이러한 문제점을 해결하고자 인원 출입 권한과 연계한 스마트폰 카메라 제어 시스템을 제안하고 설계한다.

3.1 SCPA 시스템 구성과 데이터 흐름

SCPA 시스템은 임직원, 협력사 직원들과 방문객들이 사무실에 출입하여 악의적인 목적으로 제품 도면, 사무실 배치, 생산 라인 등을 스마트폰 카메라 촬영으로 외부에 유출하는 것을 방지하기 위해 MCS 프로그램의 설치현황을 정보보안 운영 DB에 10분 간격으로 전송한다. 그러면, 전송된 MCS 프로그램 설치현황을 정보보안 관리자가 확인할 수 있다. 정보보안 관리자는 MCS 프로그램을 설치하지 않은 임직원, 협력사 직원들과 방문객들에게 온라인(SMS)으로 통보하여 MCS 프로그램 미설치를 최소화한다. 또한, 정보보안 관리자는 출입자의 업무를 정확히 분석하여 출입권한을 부여한다.

3.1.1 시스템 구성

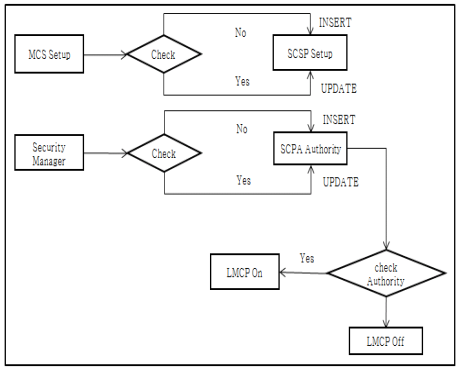
SCPA 시스템은 MCS 프로그램의 설치현황과 인원 출입 권한으로 구성된다. MCS 프로그램의 설치현황은 임직원, 협력사 직원들과 방문객들의 스마트폰에 설치된 MCS 프로그램 설치현황이 MSSQL DB에 저장된다. SCPA 시스템의 Interface Module은 MCS 프로그램 설치현황이 저장된 MSSQL DB의 데이터를 수신한 후 ORACLE DB에 저장한다. ORACLE DB에 MCS 프로그램을 설치한 인원들에게 출입권한을 정보보안 관리자가 부여한다. MCS 프로그램은 출입 가능 지역에 따라 LMCP 작동을 제어한다. 이와 같은 시스템 구성은 [Fig. 2]와 같다.



[Fig. 2] SCPA System Configuration

3.1.2 데이터 흐름

SCPA 시스템의 데이터는 MCS 프로그램의 설치현황과 인원 출입권한으로 구분한다. MCS 프로그램의 설치현황은 Interface Module을 통해 10분에 한 번씩 SCPA 시스템의 설치현황 테이블로 MacAddress와 사번을 전송한 후, 조회 결과 있으면 데이터를 수정하고, 없으면 등록한다. 또한, 인원 출입권한은 정보보안 관리자가 출입자의 업무를 분석해서 출입권한을 부여한다. 이와 같은 SCPA의 데이터 흐름은 [Fig. 3]와 같다.



[Fig. 3] Data Flow of SCPA

3.2 시스템 구현

SCPA 시스템의 구현 환경은 하드웨어 영역과 소프트웨어 영역으로 구성된다. 그리고 SCPA 시스템의 프로토콜 설계를 위한 파라미터를 정의하고 모듈별 프로토콜 설계를 위한 데이터 흐름을 단계별로 구현한다.

3.2.1 모듈 환경

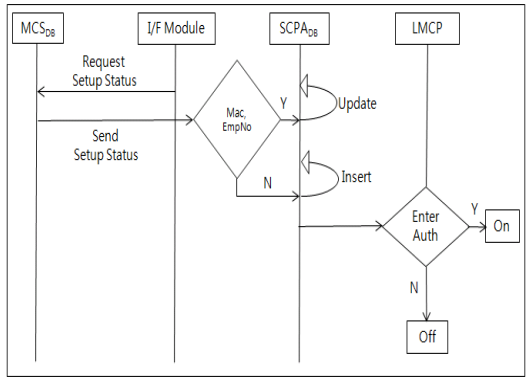
시스템 구현 환경에서 하드웨어 영역은 서버와 소프트웨어로 구성된다. 서버의 운영체제는 Window7이고, 데이터베이스는 MSSQL과 ORACLE이다. 소프트웨어는 Weblogic, Java, Jsp이다. 이와 같은 SCPA 시스템의 구현 환경과 모듈은 <Table 1>과 같다.

〈Table 1〉 SCPA Implementation Environments and Modules

Div.	Component		Qty	Model
H/W	SERVER	CPU	1	Intel Core i7-2670QM
		Memory	1	8GB
S/W	OS	Window7 Enterprise Edition 64bit		
	WAS	Weblogic8.1.6		
	Language	Jdk1.4, Jdk1.6		
	DataBase	MSSQL2008, Oracle 10g		

3.2.2 모듈 흐름

SCPA 시스템을 구현하기 위해서 4개의 모듈이 필요하다. 첫 번째로 MCS 프로그램 설치현황 데이터를 SCPA 시스템의 설치현황 테이블로 전송하는 모듈이다. 두 번째로 MCS 프로그램 설치현황을 관리하는 모듈이다. 세 번째로 인원 출입권한을 관리하는 모듈이다. 네 번째로 정보보안 관리자가 부여한 출입권한과 출입지역을 비교해서 LMCP 기능을 작동시키는 모듈이다. SCPA 시스템의 모듈 흐름은 [Fig. 4]와 같다.



[Fig. 4] Module Flow of SCPA

3.2.3 파라미터

인원 출입권한과 연계한 스마트폰 카메라 제어 시스템의 프로토콜에서 사용할 파라미터는 <Table 2>와 같이 정의한다.

〈Table 2〉 Parameters of SCPA

Code	Description
MCSDBSERVER, MCSDB	Mobile Control System DB Server, DB
InfArr1	Interface Module Array
EmpNo	Employee Number
Name	Name
MacAddress	Mobile Mac Address
Device	Mobile Sequence
Factory	Factory Code
Dept	Department
MobileNo	Mobile Number
Status	Mobile Use Status
SearchText	Search MCS Setup Status Text
ResultArr1	Result Array
ResultStr1	Entrance User
SCPADBSERVER, SCPADB	SCPA DB Server, DB
EnterArr1	Entrance Auth. Array
h(•)	One-way Hash Function

3.2.4 모듈별 프로토콜

SCPA 시스템의 4개 모듈 프로토콜은 다음과 같은 순서로 구현한다.

■ Interface 모듈 프로토콜

Interface 모듈은 MCS 프로그램 설치현황 데이터를 Interface Module을 이용해서[13] $SCPA_{DB}$ 설치현황 테이블로 전송하는 프로토콜이다. MCS 설치현황 테이블 전송 프로토콜은 사번과 MacAddress를 비교해서 있으면 수정, 없으면 등록한다. MCS 프로그램 설치현황 Interface 모듈 프로토콜의 단계별 실행 내용은 다음과 같다.

- 1단계 : Interface Module은 MCSDB에 MCS 프로그램 설치현황을 조회한 후 InfArr1에 저장한다.
  InfArr1= (h(EmpNo), Name, MacAddress, Device, Factory, Dept, MobileNo, Status)
- 2단계 : Interface Module의 InfArr1에 저장된 사번과 MacAddress로 SCPA 시스템의 MCS 프로그램 설치현황 테이블을 비교한다. InfArr1에 저장된 사번과 MacAddress가 SCPA 시스템의 MCS 프로그램 설치현황 테이블에 없으면 InfArr1에 저장된 사번, MacAddress, Device, Factory, Dept, MobileNo, Status를 추가한다. InfArr1에 저장된 사번과 MacAddress가 SCPA 시스템의 MCS 프로그램 설치현황 테이블에 있으면 InfArr1에 저장된 사번과 MacAddress를 조건값으로 Name, Device, Factory, Dept, MobileNo, Status를 수정한다.

■ 조회 모듈 프로토콜

조회 모듈은 $SCSP_{DB}$ 설치현황 테이블로 전송된 MCS 설치현황을 조회한다. MCS 설치현황을 조회하는 Keyword는 부서, 이름, 사번 등이다. SCPA 시스템에서 MCS 프로그램 설치현황 조회 모듈 프로토콜의 단계별 실행 내용은 부서, 이름, 사번 등으로 $SCSP_{DB}$를 검색해서 MCS 프로그램 설치현황을 ResultAttr1에 저장한다.

(Dept, Name, EmpNo) => $SCPA_{DB}$
ResultArr1 = (EmpNo, Name, MacAddress, Device, Factory, Dept, MobileNo, Status)

■ 인원 출입 권한 조회 모듈 프로토콜

인원 출입 권한 조회 모듈은 SCPA 시스템의 인원 출입 권한을 관리하는 프로토콜이다. 정보보안 관리자는 출입권한을 조회한 후 출입자의 정확한 업무를 파악해서 출입권한을 부여 또는 회수한다. SCPA 시스템의 인원 출입 권한을 관리 모듈 프로토콜의 단계별 실행 내용은 아래와 같다.

- 1단계 : 정보보안 관리자는 이름, 사번으로 $SCPA_{DB}$를 검색해서 출입인원을 ResultStr1에 저장한다.
  (SearchText) => $SCPA_{DB}$
  ResultStr1 = (EmpNo, Name, Dept, MobileNo, EnterArr)
- 2단계 : 정보보안 관리자는 검색된 출입 인원의 출입권한을 확인한 후 추가 또는 삭제한다.
  if(Incorrect Entrance Auth is exist) =>
  Delete Entrance Auth from $SCPA_{DB}$
  if(Correct Entrance Auth is not exist) =>
  Insert Entrance Auth from $SCPA_{DB}$

■ LMCP 작동 모듈 프로토콜

MCS 프로그램은 정보보안 관리자가 부여한 출입권한과 출입지역을 비교해서 LMCP를 작동시킨다. 정상적인 LMCP의 작동과 LMCP의 미작동 이력을 $SCPA_{DB}$에 저장한다. LMCP 작동 모듈 프로토콜의 단계별 실행 내용은 다음과 같다.

- 1단계 : 출입 인원의 스마트폰에 설치된 MCS프로그램은 $SCPA_{DB}$에 저장된 출입 인원의 출입 권한을 조회한다.
  (MCS Check Entrance Auth) => $SCPA_{DB}$

• 2단계 : $SCPA_{DB}$에 출입인원의 출입 권한이 있으면 LMCP를 작동시키고, 출입 권한이 없으면 LMCP를 작동시키지 않는다.

if(Entrance Auth is exist) =>
LMCP working
if(Entrance Auth is not exist) =>
LMCP not working

• 3단계 : LMCP의 작동, 미작동 이력을 $SCPA_{DB}$에 저장한다.

(EmpNo, Wdate, Ent_Area) => $SCPA_{DB}$

4. 비교분석

본 논문에서 제안한 SCPA 시스템 분석 방법은 MCS 프로그램 설치현황 중 2대 이상의 스마트폰을 보유한 임직원 3명, 협력사 직원 3명과 MCS 프로그램을 설치한 방문객 3명을 대상으로 LMCP의 작동여부를 분석하고 LMCP를 이용해서 저장된 제품도면, 사무실 배치, 생산라인 등을 확인한다. 그리고 방문객의 MCS 프로그램 설치로 인해 감소한 스마트폰 카메라 봉인 스티커 구입비용을 분석한다.

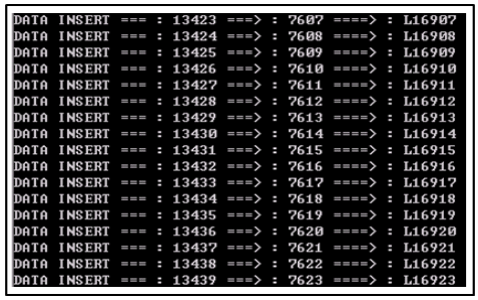
4.1 분석환경

SCPA 시스템의 분석 대상은 사무직·생산직·협력업체까지 포함한 직원 수가 12,000명이 넘는 L사를 선정했다. L사를 선정한 이유는 다양한 정보유출 관리시스템과 인원 출입 관리시스템이 구축되어 있고 제품 생산과 업무 협의를 위해 많은 방문객들이 출입하기 때문이다. SCPA 시스템의 분석을 위해 사용된 MCS 프로그램 설치현황 데이터, MCS 프로그램의 LMCP의 작동이력 데이터와 방문객의 출입현황 데이터이다.

인원 출입 권한과 연계한 스마트폰 카메라 제어시스템을 4가지 모듈로 분석한다.

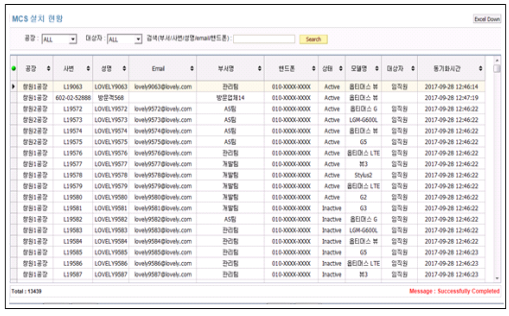
첫 번째로 MCS 시스템의 설치현황을 SCPA 시스템으로 전송하는 모듈이다.

L사에서 MCS 프로그램을 설치한 건수는 13,439건이며, 그 중에서 임직원 12,101건, 협력사 324건, 방문객 981건이다. 그리고 스마트폰을 2대 이상 등록한 인원은 총 14명이다. 그 중에서 분석인원은 임직원 3명과 협력사직원 3명, 방문객 3명이다. LMCP의 작동은 총 17,407건이며 정상 작동은 13,271건, 미 작동은 4,136건이다. MCS 프로그램 설치 현황 데이터 전송 실행화면은 [Fig. 5]와 같다.



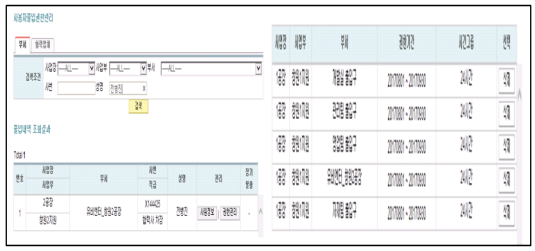
[Fig. 5] MCS Program Setup Status I/f Execution Screen

두 번째로 정보보안 관리자가 MCS 프로그램 설치 현황 조회해서 미설치자 현황을 파악하고 미설치를 최소화한다. MCS 프로그램 설치 현황 관리 실행화면은 [Fig. 6]과 같다.



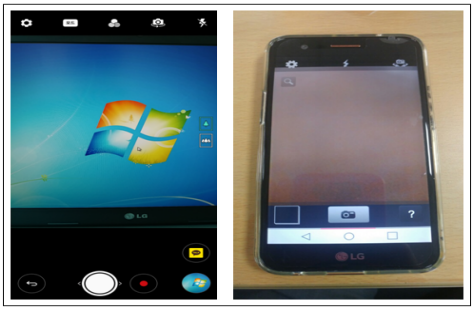
[Fig. 6] MCS Program Setup Status Data Management Execution Screen

세 번째로 정보보안 관리자는 출입하는 인원의 업무를 정확히 파악해서 출입권한을 부여한다. 정보보안 관리자의 출입권한 관리 실행화면은 [Fig. 7]과 같다.



[Fig. 7] Access Right Management of SCPA Execution Screen

네 번째, 정보보안 관리자로부터 부여 받은 출입 권한을 가진 사용자는 SCPA 시스템의 LMCP를 사용할 수 있다. 일반적인 스마트폰 카메라의 작동화면과 SCPA 시스템의 LMCP의 작동화면은 [Fig. 8]과 같다



[Fig. 8.] Operation Execution Screen of LMCP

스마트폰을 2대 이상 등록한 인원들을 분석 대상으로 선정한 후 LMCP의 작동 여부를 수치화해서 정상 작동한 사무실과 미작동한 사무실의 위치를 파악하고 LMCP를 정상 작동해서 촬영한 파일을 MCS 프로그램을 통해 전송한 현황을 분석한다. MCS 프로그램 설치 현황과 LMCP의 작동 여부 현황 등은 <Table 3>과 같다.

〈Table 3〉 Analysis MCS Status and LMCP work

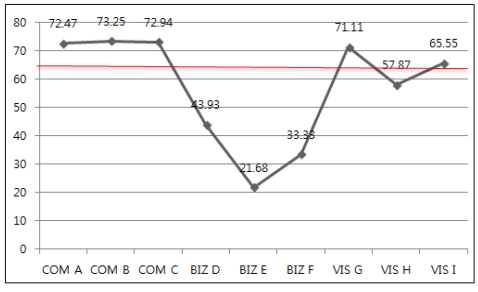
Analysis Types	Count
MCS Setup Status	13,439
More than two MCS Setup	14
LMCP Count	17,407
LMCP Work Count	13,271
LMCP Not Work Count	4,136
LMCP Work Rate	76.23%

4.2 분석 결과

분석 인원 9명의 익명성을 보장하기 위해 각각 임직원 A~C, 협력사 직원 D~F와 방문객 G~I으로 명명한다. 분석 인원 9명의 LMCP의 사용 여부를 분석한다. 분석인원 9명의 LMCP의 사용비율은 10.54%(1,836 /17,407)이고 정상 작동 비율은 65.19%(1,197/1,836)이다. 임직원 A~C의 정상 작동 비율 72.47%(258/356), 73.25%(241/329), 72.94%(240/329)이고 협력사 직원 D~F의 정상 작동 비율은 43.93%(29/66), 21.68%(18/ 83), 33.33%(30/90)이며 방문객 G~I의 정상 작동 비율 71.11%(197/277), 57.87%(125/216), 65.55%(59/90)이다. 분석 인원 9명 중 LMCP의 평균 작동 비율은 65.19%이다.

평균 작동 비율보다 높은 임직원 A~C와 방문객 G~I는 신제품 출시를 위한 업무 협의 시 도면과 업무 협의 내용을 회의록 작성을 위해 촬영한 것이다. 하지만, 협력사 직원 D가 촬영한 내용은 LMCP의 로그를 확인한 결과 출입 권한이 없는 출입지역에서 사무실 레이아웃과 무선 AP 공유기를 촬영한 것이고, 협력사 직원 E와 F는 생산 라인과 물류 차량의 화물 적재 현황을 촬영한 것이다.

협력사 직원 D~F는 출입 권한이 없는 지역에서의 촬영과 경쟁사에 생산과 관련된 정보를 유출할 위험성이 커서 협력사 대표자에게 구두 경고 조치 후 정보유출 통합모니터링 관리시스템에 악의적인 사용자로 등록하고 관리가 필요하다. 본 논문에서 제안한 인원 출입 권한과 연계한 스마트폰 카메라 제어시스템과 기존 MCS 프로그램의 LMCP의 차이점은 출입 권한이 없는 인원들은 LMCP가 비활성화되고, 출입 권한이 있는 인원들만 LMCP가 활성화된다. 사용자별 정상 작동 비율은 [Fig. 9]와 같다.



[Fig. 9] User Normal Working Rate

5. 결론

제안하는 SCPA 시스템의 목적은 기존의 스마트폰에 설치한 MCS 프로그램의 설치현황을 신속하게 파악하고 인원 출입 권한과의 정보연계를 통해 스마트폰 카메라를 통한 정보유출을 사전에 차단하는 것이다.

기업체의 임직원, 협력사 직원들과 방문객들은 스마트폰으로 사내 시스템에 접속할 수 있는 MCS 프로그램을 정보보안 관리자의 승인하에 설치해서 사용한다. MCS

프로그램은 정보보안 관리자의 승인 하에 설치되었으므로 사용상의 제약은 없다. 하지만, LMCP는 정보유출의 위험성 때문에 출입이 허가되지 않은 인원에 대해서는 작동이 되어서는 안 된다.

그래서 인원 출입 권한과 연계하여 출입이 허가된 인원만 LMCP를 작동하게 하여 정보유출을 사전에 방지할 수 있게 했다. 또한, MCS 프로그램의 LMCP를 분석 기간 중 방문객들에게도 설치해서 방문객의 사진 촬영을 방지하기 위해 부착해 주던 스마트폰 카메라 봉인 스티커 구입비용이 줄어들었다.

REFERENCES

[1] Garba, A. B., Armarego, J., Murray, D. and Kenworthy, W., “Review of the information security and privacy challenges in BYOD environments,” Journal of Information privacy and security, pp. 38-54, 2015.

[2] S. T. Kang, I. J. Jo, “Individual users based Smart Phone Remote Management System Design and Implementation,” The Korea Institute of Information and Communication Engineering, Journal of the Korea Institute of Information and Communication Engineering 16(12), pp.2675-2681, 2012.12.

[3] Onechul Na, Hangbae Chang, “Critical Intelligence Management Plan Studies for the Prevention of Corporation’s Technology Leakage,” Korean Society For Internet Information, Korean Internet Information Society Conference 17(2), pp.231-232, 2016.11

[4] S. B. Kim, B. M. Chang, “Design and Implementation of Privacy Impact Assessment Information System”, Korean Institute of Information Technology, Journal of Korean Institute of Information Technology 13(6), pp.87-104, 2015.6.

[5] D. K. Lee, J. I. Lim, “Forecast System for Security Incidents”, Journal of The Institute of Electronics and Information Engineers Vol.53, No.6, 2016.6.

[6] B. J. Jeon, D. B. Yoon, S. S. Shin, “Improved Integrated Monitoring System Design and Construction”, Journal of Korea Fusion Research Institute 7(1), pp.25-33, 2017.2

[7] Y. S. Kim, N. P., “IData Loss Prevention System having a function of Responding Data-Leaking Incidents”, THE INSTITUTE OF ELECTRONICS ENGINEERS OF KOREA, Conference on the Institute of Electronics Engineers of Korea, pp.1872-1874, 2012.6.

[8] S. G. Ryu, Y. H. Park, C. K. Kim, Y. H. Park, “Vulnerability Analysis and Countermeasure of Access Control System”, Korean Institute of Communication Sciences, Korea Telecom Society Summer Summit 2016, pp.800-801, 2016.

[9] B. M. Kim, J. M. Jeong, S. L. Yong, Taenam Cho, “A Password Scheme based on Calculation Resistant to Smudge and Shoulder Surfing Attacks”, Korea Computer Information Association, Journal of the Korean Society of Computer Information Vol.22 No.2, pp.75-76, 2014.

[10] J. W. Kim, Y. H. Lee, “Continuous-authentication Method based on the Risk Profile associated with Context-awareness to Lock Smart Devices”, KOREA INFORMATION SCIENCE SOCIETY, Journal of KIISE 43(11) Vol.20, No.8, pp.1259-1269, 2016.11.

[11] J. P. Yun, J. H. Kim, K. S. Lee, “Certificate-based SSO Protocol Complying with Web Standard”, Korea Institute of Information and Communication Engineering, Journal of the Korea Institute of Information and Communication Engineering Vol.20, No.8, pp.1466-1477, 2016.8.

[12] S. H. Seo, C. Y. Choi, G. Y. Lee, H. K. Choi, “QR Code Based Mobile Dual Transmission OTP System”, Korean Institute of Communication Sciences, The Journal of the Korean Institute of Communication Sciences Vol.38B No.5, pp.377-384, 2013.5.

[13] S. K. Hong, H. J. Jeon, Y. H. Kwon and S. H. Lee, “Extracting Information of Client Using Java Agent for Information leakage prevention”, Korean Institute of Intelligent Systems, Proceedings of the

Korea Intelligent Systems Society, pp.211-212, 2015.10.

[14] J. Y. Sung, S. D. Lee, C. J. R and S. J. Han, "Mutual Authentication Protocol using One Time Password for Mobile RFID System, Journal of the Korea Institute of Information and Communication Engineering, Vol.18, No.7, pp.1634-1642, 2014.

[15] H. J. Hwang, K. Y. Kim, I. K. Ha, "A Digital Door Lock System Using Time- Synchronous One Time Password", Journal of the Korea Institute of Information and Communication Engineering, Vol.21, No.5, pp.1027-1034, 2017.

저자소개

전 병 진(Byung-Jin Jeon) [정회원]

- 1998년 2월: 동명전문대학 전산학과 전문학사
- 2004년 2월 : 동서사이버대학교 전산학과 학사
- 2017년 2월 : 동명대학교 정보보호학과 석사
- 2017년 2월 ~ 현재 : 동명대학교 정보보호학과 박사과정

<관심분야> : 정보통신, Iot, 물리보안, 안드로이드

한 군 희(Kun-Hee Han) [종신회원]

- 2008년 8월 ~ 현재 : 백석대학교 정보통신공학부 교수

<관심분야> : 암호프로토콜, 네트워크보안, 영상처리

신 승 수(Seung-Soo Shin) [정회원]

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야> : 암호프로토콜, 빅데이터, USN, 헬스케어 보안, Iot