Regular paper | Journal of the KIECS. pp. 1003-1008, vol. 11, no. 10, Oct. 31 2016, t. 78, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2016.11.10.1003

ACL이 적용된 라우터 기반의 제한된 병원 의료정보시스템의 구현 사례

윤성자* · 김노환* · 강은홍**

The case study of implementation for a limited hospital medical information system based on ACL-applied router

Sung-Ja Yoon* · No-Whan Kim** · Eun-Hong Kang*

요 약

최근 병원들은 다양한 서비스, 진료 활성화와 질 향상을 위하여 많은 부서들로 분업화 및 세분화되면서 유기적인 협업으로 양질의 환자서비스를 제공하고 있으며, 진료정보 접근권한 제한과 환자의 개인정보 유출 방지를 위한 정보보호 시스템을 도입하여 운영하는 등 정보보호 대책도 진일보하고 있다.

본 논문에서는 정보접근을 제한하기 위하여 ACL(: Access Control List)이 적용된 라우터 기반의 가상 망을 패킷 트레이서를 이용하여 구현한 다음, 시뮬레이션을 통해서 정보의 차단 및 허용을 검증할 수 있는 제한된 병원 의료정보시스템의 구현 사례를 제시하였다.

ABSTRACT

Recently hospitals have divided into many divisions, specialized the medical service, and shown organic cooperation, all to provide patients with various and high quality medical service. They have also showed improvement in information protection by introducing an information protection system to regulate the access to patients' medical and personal information.

The purpose of this paper is to present a case study to implement of a limited hospital medical information system that can regulate the access to medical information. For this, a router-based virtual network applying an ACL(: Access Control List) to regulate access to information was made using a packet tracer.

키워드

Clinical Information, Information Security, ACL, Router, Virtual Network, Packet Tracer
진료 정보, 정보 보호, ACL, 라우터, 가상망, 패킷 트레이서

Ⅰ. 서 론

ACL(: Access Control List)은 네트워크의 접근 허용 여부를 정해놓은 목록으로 라우터의 인터페이스에 적용함으로써 라우터를 경유하는 특정 패킷을 필터링하고 출발지 주소, 목적지 주소, TCP/UDP 포트 등을

* 경동대학교 간호학부 (soyang1129@kduniv.ac.kr, nwkim@kduniv.ac.kr)
** 교신저자 : 경동대학교 간호학부
· 접 수 일 : 2016. 09. 19
· 수정완료일 : 2016. 10. 13
· 게재확정일 : 2016. 10. 24
· Received : Sep. 19, 2016, Revised : Oct. 13, 2016, Accepted : Oct. 24, 2016
· Corresponding Author : Eun-Hong Kang
School of Nursing, Kyung-Dong University,
Email : kbeebee@kduniv.ac.kr

기반으로 허가되지 않은 특정 IP 혹은 포트를 지정하여 접근을 제한한다[1].

의료기관의 궁극적인 목적은 환자의 건강관리이기도 하지만 그에 상응하는 편익성이 따라야 대상자의 만족도를 높일 수가 있다. 이 목적과 편익성이 부합하는 의료정보시스템이 의료기관과 환자들에게 절실하므로, 거점병원과 지역병원 간 의료정보에 대한 협업과 함께 접근권한을 효율적으로 제한하여 환자에 대한 의료서비스를 보장해야만 한다.

본 논문은 관련연구로 해당 논문을 검토한 후, 선행연구로 병원 의료정보시스템을 검토하였고, 본론에서는 ACL을 적용한 라우터와 각 단말기에 IP 주소를 할당한 공통 가상 망을 구현하였다. 시뮬레이션을 통해서 보안정책에 기반 한 각 부서 간 접근권한을 제한하여 의료정보의 차단 및 허용을 검증할 수 있는 ACL이 적용된 라우터 기반의 제한된 병원 의료정보 시스템의 구현 사례를 제시하였다.

II. 관련 연구

2.1 논문연구

배석찬은 사용자 그룹이 접근하고자 하는 서버에서의 환자 의무기록 사항에 대해 먼저 보안정책을 고려하여 자동적으로 키 등급을 비교하였다. 그리고 등급 생성을 저장하여, 접근하고자 하는 서버의 자료와 등급을 비교하여 더 높은 키 등급을 소유하고 있는 사용자가 서버에 있는 자료를 열람하고 기타 연산이 가능하도록 제안하였다[2].

송지은 외 3인은 신뢰성과 안전성을 보장하는 Home-Healthcare 서비스를 제공하기 위한 정보보호 요구사항 및 이슈들을 살펴본 후 이와 관련된 대안 기술들을 구체적으로 검토하였다[3].

문형진 외 4인은 정보주체의 민감한 정보 항목을 개인별 정책에 반영하고 개인에 의해 지정된 민감한 개인정보 접근에 대해 엄격하게 제한하는 프라이버시 정책 기반의 접근제어 기법을 제안하고 있다[4].

김경진, 홍승필은 e-Healthcare 환경 내 개인의 의료정보 보호를 위한 역할기반의 접근제어 시스템(HPIP : Health Privacy Information Protection)을 네 가지 주요 메커니즘(사용자 신분확인, 병원 권한확인, 진료기록 접근제어, 환자진단)으로 제안하였으며, 실 환경에서 효과적으로 활용될 수 있도록 프로토타이핑을 통해 그 가능성을 타진하였다[5].

임종우 외 4인은 환자 사생활 정보보호 및 의료정보를 공유하기 위해, 국내외 의료정보 공유현황 및 관련 국제의료정보 표준안 고찰 및 국내 의료기관의 데모그래픽 데이터를 활용해 보고 실제 국내 의료기관의 환자 데이터구조 및 특성을 분석하여 의료정보 공유시스템 구조 설계를 제안하였다[6].

윤석권, 송정영은 각 병원에서 사용하고 있는 EMR(: Electronic Medical Record)의 내용을 전자서명을 통해 객관적인 인증과 동시에 환자 개인의 정보보호에도 문제가 없는 시스템 구축에 대하여 논의하고 이를 검증하였다[7].

2.2 선행연구

2.2.1 확장 ACL

확장 ACL은 출입 통제 시 출발지 주소, 목적지 주소, 프로토콜, 포트번호 등을 검사하여 제어한다. 그림 1에 보인 바와 같이 ACL을 확인하고 없으면 패킷을 정해진 경로로 내보내도록 “허용(permit)”한다[1].

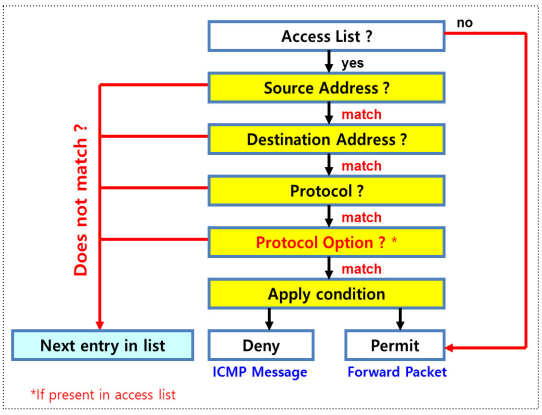


그림 1. 확장 ACL의 동작
Fig. 1 Operation of extended access list

2.2.2 제한된 병원 의료정보 시스템의 계층적 모델

병원은 환자에 대한 의료서비스를 제공하는 기관으로, 정보의 접근권한에 대한 병원의 보안정책에 따라

인가자와 비인가자를 구분하여 환자의 의료기록 및 개인정보에 접근권한을 제한해야 한다[9].

그림 2는 제한된 병원 의료정보시스템의 계층적 모델을 보여주고 있다.

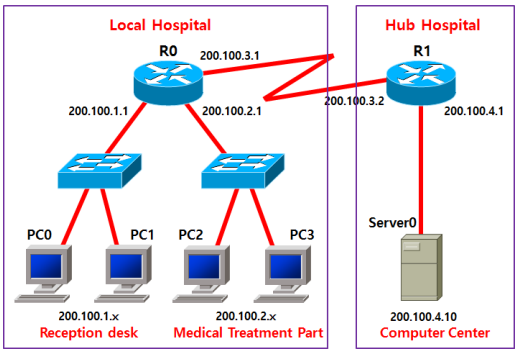


그림 2. 제한된 병원 의료정보시스템의 계층적 모델
Fig. 2 Hierarchical model of limited medical information system on hospital

거점병원과 지역병원 간 또는 각 부서 간 정보를 차단하거나 허용하도록 하기 위한 Server, Firewall, Data Storage 등의 장비가 도입되어 운용 중이지만, 접근권한에 대한 보안정책에 따라 병원 내 각 부서 및 직급별로 의료정보의 접근권한은 상이할 것이다.

지역병원의 접수처는 내원환자를 위한 수납업무, 입원등록, 주차확인, 원문복사서비스, 수가 업무 등을 수행하므로, 제한적으로 거점병원과 무관하게 독립적인 업무처리가 가능하므로 거점병원에 접근권한을 부여하지 않는 것으로 가정하였다.

진료부는 본인의 진료수입 및 담당환자 현황에 접근 가능하고 담당환자에 관련하여 과거력 및 현 상황을 볼 수 있는 권한이 있고, 진료와 관련된 증명서 발급, 임상검사결과 조회 등을 할 수 있으므로 거점병원에 접근권한이 있다고 가정하였다.

전산센터는 병원의 모든 정보를 관리하고 프로그램을 개발 운영하며 시스템을 유지 보수하는 부서로서, 보안유지가 생명이며 지역병원에 대한 모든 접근권한을 갖고 있다고 가정하였다.

III. 본 론

병원 의료정보시스템의 계층적 모델에 기반 한 가상 망을 구현하고, 라우터에 ACL을 구현한 후, 시뮬레이션을 통해서 정보의 제한을 검증할 수 있는 제한된 병원 의료정보시스템의 구현사례를 제시하였다.

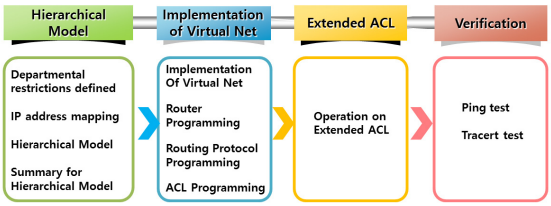
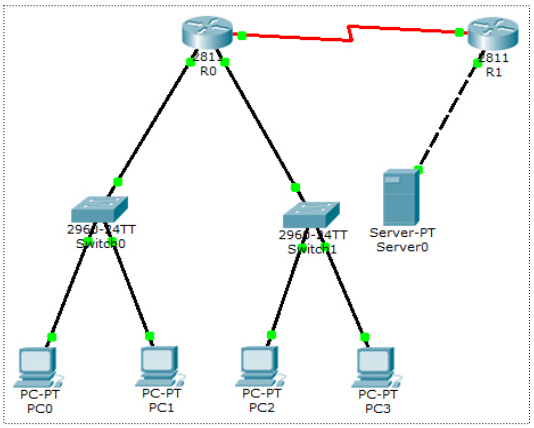


그림 3. 제한된 병원 의료정보 시스템의 구현사례
Fig. 3 The case for implementation of limited medical information system on hospital

3.1 가상망 구성

접근권한의 제한을 검증하기 위하여, 그림 2와 같은 계층적 모델을 기반으로 그림 4와 같은 가상 망을 패킷 트레이서로 구현하고 RIP(: Routing Information Protocol) 라우팅 프로토콜을 적용하였다[8].



IP/suffix	port	Equip.	IP/suffix	port	Equip.
200.100.1.1 /24	fa0/0	R0	200.100.2.2 /24		PC2
200.100.2.1 /24	fa0/1	R0	200.100.2.3 /24		PC3
200.100.3.1 /24	s0/2/0	R0	200.100.3.2 /24	s0/2/0	R1
200.100.1.2 /24		PC0	200.100.4.1 /24	fa0/0	R1
200.100.1.3 /24		PC1	200.100.4.10 /24		Server0

그림 4. 가상 망 구현
Fig. 4 Implementation of virtual networks

3.2 ACL이 적용된 시뮬레이션 결과

ACL은 ACL을 정의하는 명령어와 인터페이스를 설정하는 명령어로 구성된다.되며, 명령어 포맷과 예시는 다음과 같다.

R1(config)#access-list <list-number> {permit |deny} <protocol> source [mask] destination [mask] [operator port]

명령어에서, list-number는 100-199까지의 번호를 사용하고 조건에 맞는 트래픽을 permit할지 deny할지 결정한다. 또한, TCP, UDP, IP, ICMP 등 filtering을 할 프로토콜을 정의하며, source 및 destination address를 지정한 후 목적지 TCP/UDP 포트 이름 및 번호를 지정한다.

R2(config)#access-list 110 deny tcp 200.101.52.0 0.0.0.255 129.29.31.0 0.0.0.255 eq 80

(1) 시나리오 1

그림 5는 그림 4의 가상 망에서, 접수처 PC0 및 PC1에서 진료부 PC2 및 PC3, 전산센터 Server0와 다른 네트워크에 접근할 수 없도록 하고, 전산센터 Server0에서는 모든 부서의 PC에 접근이 가능하도록 지역병원 라우터 R0에 ACL을 적용한 예이다.

```
R0(config)#access-list 100 deny icmp host 200.100.1.2 any echo
R0(config)#access-list 100 remark request deny and echo permit
R0(config)#access-list 100 permit ip any any
R0(config)#int f0/0
R0(config-if)#ip access-group 100 in
R0(config-if)#ex
R0(config)#do sh access-list
Extended IP access list 100
    deny icmp host 200.100.1.2 any echo
    permit ip any any
```

그림 5. R0의 확장 ACL 적용
Fig. 5 Applying of extended ACL on R0

그림 6은 시뮬레이션 결과로서, 접수처 PC0에서 거점병원 라우터 R1에만 ping을 보낼 수 없도록 지역병원 라우터 R0에 ACL을 적용한 경우로, PC0는 ping이 되지 않고 다른 PC는 ping이 정상적으로 이루어지므로 가정한 대로 거점병원에 접근권한을 부여되지 않음을 확인 하였다.

```
Command Prompt
PC>ping 200.100.4.10

Pinging 200.100.4.10 with 32 bytes of data:

Reply from 200.100.1.1: Destination host unreachable.
Reply from 200.100.1.1: Destination host unreachable.
Reply from 200.100.1.1: Destination host unreachable.
Reply from 200.100.1.1: Destination host unreachable.

Ping statistics for 200.100.4.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 200.100.2.2

Pinging 200.100.2.2 with 32 bytes of data:

Reply from 200.100.1.1: Destination host unreachable.
Reply from 200.100.1.1: Destination host unreachable.
Reply from 200.100.1.1: Destination host unreachable.
Reply from 200.100.1.1: Destination host unreachable.

Ping statistics for 200.100.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(a) PC0에서

```
Command Prompt
SERVER>ping 200.100.1.2

Pinging 200.100.1.2 with 32 bytes of data:

Reply from 200.100.1.2: bytes=32 time=124ms TTL=126
Reply from 200.100.1.2: bytes=32 time=125ms TTL=126
Reply from 200.100.1.2: bytes=32 time=125ms TTL=126
Reply from 200.100.1.2: bytes=32 time=125ms TTL=126

Ping statistics for 200.100.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 124ms, Maximum = 125ms, Average = 124ms

SERVER>ping 200.100.2.3

Pinging 200.100.2.3 with 32 bytes of data:

Reply from 200.100.2.3: bytes=32 time=97ms TTL=126
Reply from 200.100.2.3: bytes=32 time=93ms TTL=126
Reply from 200.100.2.3: bytes=32 time=104ms TTL=126
Reply from 200.100.2.3: bytes=32 time=109ms TTL=126

Ping statistics for 200.100.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 109ms, Average = 100ms
```

(b) Server0에서

그림 6. ACL의 시뮬레이션 결과
Fig. 6 The Simulation results of ACL

(2) 시나리오 2

그림 7은 그림 4의 가상 망에서, 서버가 외부로부터 ICMP 공격을 받는 경우, 수신 ICMP를 차단하여 공격을 방지하고, 접수처 PC0에서 오는 트래픽이 거점병원 FTP 서버 '200.100.4.10'에 접근하는 것을 차단하며, 접수처 PC1에서 오는 트래픽이 거점병원 라우터 R1의 '200.100.3.2'로 Telnet 접근을 차단하고, 네트워크 '200.100.2.0'에서는 인터넷 접속이 불가하여 거점병원 웹서버 '200.100.4.10' 접근을 차단하도록 거점병원 라우터 R1에 ACL을 적용한 예이다.

```
R1(config)#access-list 110 deny icmp any 200.100.4.0 0.0.0.255 echo
R1(config)#access-list 110 deny tcp host 200.100.1.2 host 200.100.4.10 eq 20
R1(config)#access-list 110 deny tcp host 200.100.1.2 host 200.100.4.10 eq 21
R1(config)#access-list 110 deny tcp host 200.100.1.3 host 200.100.3.2 eq 23
R1(config)#access-list 110 deny tcp 200.100.2.0 0.0.0.255 host 200.100.4.10 eq 80
R1(config)#access-list 110 permit ip any any
R1(config)#int s0/2/0
R1(config)#ip access-group 110 in
R1(config)#ex
R1#
R1(config)#enable password admin
R1(config)#line vty 0 4
R1(config-line)#password admin
R1(config-line)#login

R1(config)#do sh access-list
Extended IP access list 110
    deny icmp any 200.100.4.0 0.0.0.255 echo
    deny tcp host 200.100.1.2 host 200.100.4.10 eq 20
    deny tcp host 200.100.1.2 host 200.100.4.10 eq ftp
    deny tcp host 200.100.1.3 host 200.100.3.2 eq telnet
    deny tcp 200.100.2.0 0.0.0.255 host 200.100.4.10 eq www
    permit ip any any (2 match(es))
R1(config)#
```

그림 7. R1의 확장 ACL 적용
Fig. 7 Applying of extended ACL on R1

그림 8은 시뮬레이션 결과로서, 거점병원 Server0가 외부로부터 ICMP(: Internet Control Message Protocol) 공격을 받고 있는 경우, 수신 ICMP를 차단하여 공격을 방지하고, 접수처 PC0에서는 거점병원 Server로 ping이 불가하며, 지역병원의 모든 부서 PC에서 거점병원 Server0로 ping이 불가한 반면, 거점병원 Server0에서는 모든 PC로 ping이 정상적으로 이루어지고 있으므로 가정한대로 지역병원에 대한 모든 접근권한을 가지고 있음을 확인 하였다.

```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 200.100.4.10

Pinging 200.100.4.10 with 32 bytes of data:

Reply from 200.100.3.2: Destination host unreachable.
Reply from 200.100.3.2: Destination host unreachable.
Reply from 200.100.3.2: Destination host unreachable.
Reply from 200.100.3.2: Destination host unreachable.

Ping statistics for 200.100.4.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Packet Tracer SERVER Command Line 1.0
SERVER>ping 200.100.1.2

Pinging 200.100.1.2 with 32 bytes of data:

Reply from 200.100.1.2: bytes=32 time=140ms TTL=126
Reply from 200.100.1.2: bytes=32 time=125ms TTL=126
Reply from 200.100.1.2: bytes=32 time=125ms TTL=126
Reply from 200.100.1.2: bytes=32 time=111ms TTL=126

Ping statistics for 200.100.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 111ms, Maximum = 140ms, Average = 125ms

SERVER>
```

그림 8. ACL의 시뮬레이션 결과
Fig. 8 The Simulation results of ACL

또한, 접수처 PC0에서 오는 트래픽은 거점병원 FTP 서버 '200.100.4.10'에 접근이 차단되고 다른 부서의 PC에서 오는 트래픽은 ftp 접속이 정상적으로 이루어짐도 확인 하였다. 역시 가정한 대로 거점병원에 접근권한을 부여되지 않음을 확인 하였다.

Ⅳ. 결 론

본 논문에서는 병원 의료정보시스템의 계층적 모델에 기반 한 가상 망을 구현한 다음, 라우터에 ACL을 구현한 후 시뮬레이션을 통해서 정보에 대한 접근제한을 검증할 수 있는 제한된 병원 의료정보시스템의 구현사례를 제시하였다.

제시된 구현 사례는 4개의 호스트와 2개의 라우터 및 1개의 Server를 갖는 4개의 네트워크로 구성한 제한된 병원 의료정보시스템의 계층적 모델을 기반으로, 지역병원과 거점병원의 접수처・진료부・전산센터의 기능 중 대표적 접근권한을 예시한 후, 이를 검증하기 위해 라우터 R0와 R1에 ACL을 설정하였다.

ACL이 설정된 공통 가상 망의 라우터에서 show access-list 명령을 실행하여 ACL 설정을 확인 한 후, 각 PC와 Server에서 ping, telnet, ftp 등을 통해 부서별 접근권한을 각각 검증하였다

시뮬레이션 결과, ACL을 라우터 인터페이스에 적용함으로써 특정 패킷을 필터링하고 출발지 주소, 목적지 주소, TCP/UDP 포트 등을 기반으로 허가되지 않은 특정 IP 혹은 포트를 지정하여 차단함으로서 공통 가상 망이 정상적으로 동작함을 확인하였다[10].

따라서, 구현 사례는 개인에게 가장 민감한 의료정보가 유출되지 않도록 병원의 보안정책이 정해졌다는 가정 하에, 계층적 모델을 통해 의료정보시스템과 ACL을 검토한 다음 상호 간에 역할을 연계한 후, 검증과정을 통해 ACL이 적용된 라우터가 병원 의료정보시스템에서도 적용될 수 있음을 시뮬레이션을 통해 보여주고 있다[11].

그러나 ACL이 설정된 라우터 만으로는 한계가 분명히 있으므로 방화벽 등을 구축하여 보다 안전한 보안대책이 강구되어야 한다.

향후, 제시된 ACL이 설정된 라우터 기반의 제한된 병원 의료정보시스템의 구현 사례를 실무에 적용하기

위해서는 방화벽 구축과 함께 병원의 원무 및 일반관리, 처방, 검사 및 진료 지원 관리, 경영정보 관리, 영상의 저장과 전달, 환자의무기록 등 병원 전반에 걸친 각 부서의 기능과 접근권한, 보안정책 등을 보다 세분화하여 체계화할 필요가 있다.

Reference

[1] J. Kim, H. Park, S, Jang, and N. Kim, "The case study for verification of ACL(:Access Lis)," *Conf. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 2, Sokcho, Korea, Nov. 2015, pp. 164-167.

[2] S. Bae, "Personal Information Security in Hospital Information System Using Degree of Key," *Conf. of Korea Information Processing Society,* Iksan, Korea, Nov. 2005, pp. 587-590.

[3] J. Song, S. Kim, M. Chung, and K. Chung, "*A Review for information protection of Home-Healthcare Service*," *Review of Korea Institute of Information Security & Cryptology,* vol. 16, no. 6, Dec. 2006, pp. 56-63.

[4] H. Mun, K. Kim, N. Um, Y. Li, and S. Lee, "Effective Access Control Mechanism for Protection of Sensitive Personal Information," *J. of Korea Information and Communications Society*, vol. 32, no. 7, July 2007, pp. 667-673.

[5] K. Kim and S. Hong, "Privacy Information Protection Model in e-Healthcare Environment," *J. of Korean Society for Internet Information*, vol. 10, no. 2, Apr. 2009, pp. 29-40.

[6] J. Lim, E. Jung, B. Jeong, D. Park, and T. Whangbo, "A Study for Sharing Patient Medical Information with Demographic Datasets," *J. of the Institute of Electronics and Information Engineers*, vol. 51, no. 10, Oct. 2014, pp. 2262-2270.

[7] S. Youn and J. Song, "EMR Management system for the patient management," *J. of Engineering Paichai University, Korea,* vol. 8, no. 1, Mar. 2006, pp. 79-85.

[8] N. Kim, "The case study to verify of a network based on router applying an ACL(:Access Lis)," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 5, May 2016, pp. 491-497.

[9] Y. Jeun, "The Medical Information Protection and major Issues," *J. of the Korea Society of Computer and Information,* vol. 17, no. 12, Dec. 2012, pp. 251-258.

[10] W. Seo and M. Jun, "A Study on Security Hole Attack According to the Establishment of Policies to Limit Particular IP Area," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 5, no. 6, Dec. 2010, pp. 625-630.

[11] J. Choi, "Utilization value of medical Big Data created in operation of medical information system," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 10, no. 12, Dec. 2015, pp. 1403-1410.

저자 소개

윤성자(Sung-Ja Yoon)

1998년 가톨릭대학교 보건대학원 보건학과 졸업(보건학석사)
2015년 강원대학교 대학원 간호학과 졸업(간호학박사)
2016～현재 : 경동대학교 간호학부 교수
※ 관심분야 : 임상의료정보

김노환(No-Whan Kim)

1978년 숭실대 전자공학과 졸업
1983년 연세대 산업대학원 졸업
2002년 강원대학교 대학원 전자공학과 졸업(공학박사)
1993～현재 : 경동대학교 간호학부 교수
※ 관심분야 : 컴퓨터네트워크

강은홍(Eun-Hong Kang)

2000년 가톨릭대학교 보건대학원 보건학과 졸업(보건학석사)
2016년 가톨릭대학교 대학원 보건학과 졸업(보건학박사)
2016～현재 : 경동대학교 간호학부 교수
※ 관심분야 : 의료정보