의료 정보유출 방지를 위한 네트워크 이중 접근통제 모델 연구

최경호*, 강성관**, 정경용***, 이정현****

A Study of Network 2-Factor Access Control Model for Prevention the Medical-Data Leakage

Kyong-Ho Choi*, Sung-Kwan Kang, Kyung-Yong Chung***, Jung-Hyun Lee****

요 약 시스템 및 네트워크에 설치/운용되는 의료자산보호 솔루션 중 네트워크 접근통제 시스템은 내부 네트워크에 접근하는 정보통신 디바이스의 안전성을 검증한 후 자원을 사용하게 하는 프로세스를 제공한다. 그러나 인가된 정보통신 디바이스의 위장 및 허가된 사용자의 이석 시간을 이용한 비인가 사용 등으로 내부 네트워크에 대한 의료 정보 절취 위협은 여전히 존재하고 있고, 장시간 운영되는 정보통신 디바이스의 경우는 사용자가 인지하지 못하는 시간대에 악성코드 감염에 의한 외부 네트워크 임의 접속 및 의료 정보유출도 발생할 수 있기 때문에 이러한 위협을 차단하기 위한 보안 대책이 필요하다. 따라서 본 논문에서는 의료 정보유출 방지를 위해 현행 네트워크 접근통제 시스템을 개선하여 적용한 네트워크 이중 접근통제 모델을 제시한다. 제안한 네트워크 이중 접근통제 모델은 사용자가 실제 조직 내부에 위치하고 있어 인가된 정보통신 디바이스를 활용하는 때에만 내부 네트워크 접속을 허용한다. 그러므로 비인가자의 내부 네트워크 접근을 차단하고, 허가된 사용자 부재 시의 불필요한 외부 인터넷 접속을 차단함으로써 의료 정보를 보호할 수 있는 안전한 의료자산 환경을 제공한다.

주제어 : 접근통제, 정보보호, 식별, NAC, 의료자산보호

Abstract Network Access Control system of medical asset protection solutions that installation and operation on system and network to provide a process that to access internal network after verifying the safety of information communication devices. However, there are still the internal medical-data leakage threats due to spoof of authorized devices and unauthorized using of users are away hours. In this paper, Network 2-Factor Access Control Model proposed for prevention the medical-data leakage by improving the current Network Access Control system. The proposed Network 2-Factor Access Control Model allowed to access the internal network only actual users located in specific place within the organization and used authorized devices. Therefore, the proposed model to provide a safety medical asset environment that protecting medical-data by blocking unauthorized access to the internal network and unnecessary internet access of authorized users and devices.

Key Words : Access Control, Information Security, Identification, NAC, Medical Asset Protection

1. 서론

정보통신기술이 발달되어 다양한 정보가 대량으로 수집/저장/분석/활용되는 오늘날의 정보화 사회에서는 IT 융합기술을 통한 정보 활용성 증대뿐만 아니라 조직 내

본 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2012-0004478).
*경기대학교 산업기술보호특화센터 연구교수
**인하대학교 컴퓨터정보공학과 박사과정
***상지대학교 컴퓨터정보공학부 교수(교신저자)
****인하대학교 컴퓨터정보공학과 교수
논문접수: 2012년 7월 1일, 1차 수정을 거쳐, 심사완료: 2012년 7월 20일

핵심정보를 보호하는 활동 역시 꾸준히 추진되고 지속 발전되어야 한다. 이미 다수 발생한 정보유출로 인한 조직의 활동 중지 경험과 나날이 증가하고 있는 해킹 및 악성코드 위협은 이의 필요성을 더욱 부각시켜준다. 이와 같은 맥락에서 의료자산보호를 위한 얼굴인식[13], 정보유출형 악성코드[8], 지능화된 피싱과[18] 같은 공격 유형과 침해사고 조기 대응[5], 통합보안관제 기법 향상[3] 등과 같은 대응 메커니즘에 관한 연구가 계속 진행되고 있다. 이들은 다양한 시스템 및 네트워크 의료자산보호 솔루션을 기반으로 사이버 위협으로부터 의료 정보를 보호하기 위한 진보적인 보안구조를 제시하고 있으며, 기존 대응 메커니즘의 발전적 양상도 포함하고 있다.

시스템 및 네트워크에 설치/운용되는 의료자산보호 솔루션 중 네트워크 접근통제 시스템은 내부 네트워크에 접근하는 정보통신 디바이스의 안전성을 검증한 후 자원을 사용하게 하는 프로세스를 제공한다[2]. 이를 통해 악의적 공격자에 의한 정보절취 공격과 악성코드 확산으로 인한 비의도적 정보 유출로부터 조직 내 중요정보를 보호할 수 있다[13]. 그러나 이와 같은 장점에도 불구하고, 인증된 정보통신 디바이스로 위장하여 내부 네트워크에 접속 및 정보절취를 시도하거나, 인증된 정보통신 디바이스의 악성코드 감염에 의한 외부 네트워크 임의 접속을 차단하기가 어려운 등의 문제점도 있다. 그러므로 네트워크 접근통제 시스템 운영과정에서 이러한 문제점이 발생하게 되는 원인을 식별하고, 이를 개선/보완하기 위한 대책을 마련하여, 의료 정보보호를 위한 보안구조를 보다 더 강건히 할 필요성이 제기된다.

따라서 본 논문에서는 의료 정보 유출 방지를 위해 현행 네트워크 접근통제 시스템을 개선하여 적용한 네트워크 이중 접근통제 모델을 제시한다. 이를 위해 2장에서는 네트워크 접근통제 시스템과 사용자 식별 및 인증수단에 대해 살펴보고, 3장에서 의료 정보유출 방지를 위한 네트워크 이중 접근통제 모델을 제시한다. 4장은 모델의 구현과 평가를 기술하고 5장에서는 결론에 대해서 기술한다.

2. 관련연구

2.1 네트워크 접근통제 시스템

네트워크 접근통제 시스템은 보안 위협에 노출 및 비인가된 정보통신 디바이스의 내부 네트워크 접속을 차단하는 역할을 수행한다[13]. 가트너(Gartner)는 네트워크 접근통제 시스템 참조 모델의 순환운영절차를 제시하였으며[19], 이를 정리하면 다음 <표 1>과 같다.

〈표 1〉 네트워크 접근통제 시스템의 순환운영절차

단계	세부 내용
정책 설정	보안 설정 시스템・네트워크・사용자 프로그램 접근
기준 수립	시스템・네트워크・사용자 프로그램 설정 패치 상태 악성코드 차단 수준 운영에 필요한 프로세스 정의
접근 통제	차단 격리 제한적 접근 허용
위험 완화	시스템・네트워크・사용자 프로그램 설정 변경 패치 설치 악성코드 치료 프로그램 최신화 보수(repair)
상태 감시	정보통신 디바이스의 상태 변화 네트워크 및 정보통신 디바이스의 이상 탐지
위험 수용	연결 해제 전송 데이터 폐기(drop traffic) 제한적 접근 허용

네트워크 접근통제 시스템 이용 시 정보통신 디바이스의 인가 여부를 판단하는 인증 방식은 802.1X, MAC (media access control) address 그리고 Web 기반으로 운영되며[7], 이를 이용해 내부 네트워크 구간에서 신뢰성 있는 통신이 가능하다. 그러나 인가된 정보통신 디바이스의 위장 및 허가된 사용자의 이석 시간을 이용한 비인가 사용 등으로 내부 네트워크에 대한 정보절취 위협은 여전히 존재하고 있으며, 이에 따라 추가적인 대책의 수립 및 적용을 통한 보안 강화 노력이 요구된다.

또한 사용자의 요구 또는 업무 특성에 따라 장시간 운영되는 정보통신 디바이스의 경우, 사용자가 인지하지 못하는 시간대에 악성코드 감염에 의한 외부 네트워크 임의 접속 및 정보 유출이 발생할 수 있기 때문에 이를 차단하기 위한 의료 보안 대책도 필요하다.

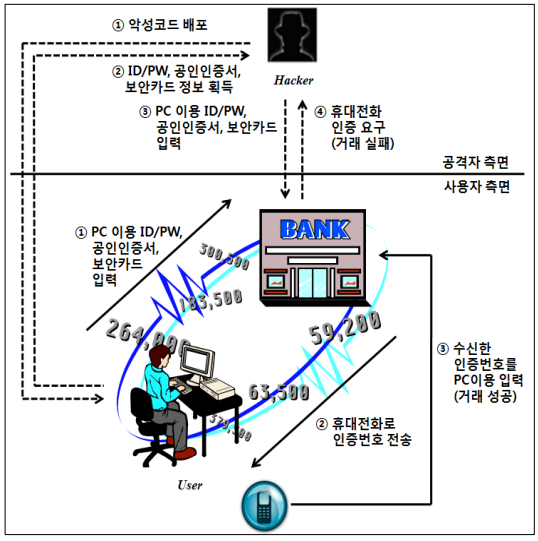
이러한 사항들은 다양한 유무선 디바이스를 이용하여 생체 및 의료정보를 교환하는 의료 정보 네트워크에서도 동일하게 요구된다. 특히, 의료정보는 개인의 병력, 증상, 가족력 등 민감한 부분들이 많기 때문에 더욱 비인가자

로부터의 허가되지 않은 열람이 발생되어서는 안된다. 따라서 허가된 사용자가 인가된 디바이스를 이용하여 내부 네트워크에 접근하는 것과 같이 수립된 의료 보안정책이 올바르게 집행되고 있는지를 확인하고, 이상징후 발생 시 즉시 차단하여 외부로 민감한 의료정보가 유출되는 것을 차단할 필요가 있다. 본 논문에서는 이와 같은 필요성을 인식하고 이중 접근통제 모델을 구축 및 실험한다.

2.2 사용자 식별 및 인증

사용자 식별 및 인증은 접근통제의 일부분으로 진행되며, 성공적으로 이행될 시 허가된 사용자임을 확신하고 내부 네트워크 접속 등의 권한을 부여해줄 수 있다. 이러한 절차는 사이버 공간의 익명성과 비대면성으로 인한 개인과 사회의 피해가 증가하고[11] 있는 오늘날의 현실에서 필수적으로 요구된다.

사용자 식별과 인증에 사용되는 방법은 특성에 따라 분류할 수 있다[9]. 비밀번호, 전화번호 등과 같이 알고 있는 사실 중심적인 지식 기반, 스마트카드 등의 소지 기반 그리고 홍채, 정맥 등의 존재 기반 등으로 분류된다. 각각의 분류된 방법은 사용자 식별과 인증에 활용 시 소요 비용의 고저, 유일성을 지니게 되어 복제 난이, 분실 시 실사용자도 접근 권한을 상실하게 된다는 등의 장단점이 있다.

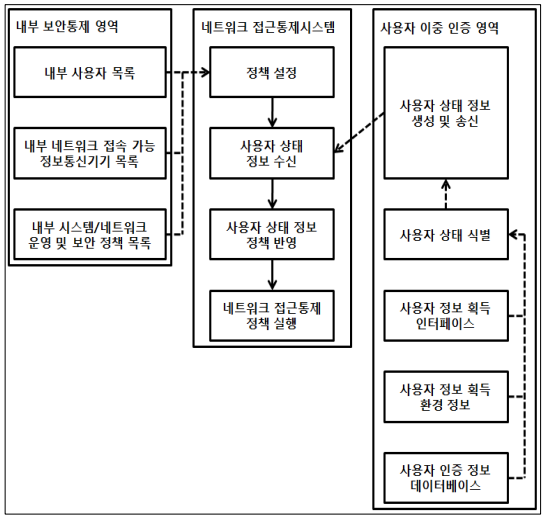


[그림 1] 금융 분야에 적용된 이중 인증 예시

최근에는 사용자 식별 및 인증에 사용되는 방법의 단점을 보완하고, 보안성을 강화하기 위해 두 가지 이상의 방법을 이용하여 접근 통제를 시행하는 연구가 지속 추진되고 있다[6][12][15]. [그림 1]은 금융 분야에서 사용하고 있는 이중 인증으로 인한 보안성 강화 효과 예시를 보여준다. 따라서 내부 네트워크 접근 및 차단을 위해 수립/적용하고 있는 의료 보안정책과 이를 구현하는 기술 및 세부 기능의 명세도 이러한 추세를 반영하여 이중 인증이 가능하도록 발전되어야 한다.

3. 의료 정보유출 방지를 위한 네트워크 이중 접근통제 모델

본 논문에서 제안하는 의료 정보유출 방지를 위한 네트워크 이중 접근통제 모델은 내부 사용자의 조직 내 위치 여부를 확인하여 실제 허가된 사용자와 해당 사용자에게 인가된 정보통신 디바이스의 내부 네트워크 접속을 허용해준다. 이를 위해 의료 정보유출 방지를 위한 사용자 이중 인증시스템이 네트워크 접근통제 시스템과 연동 운영되며 [그림 2]와 같이 표현된다.

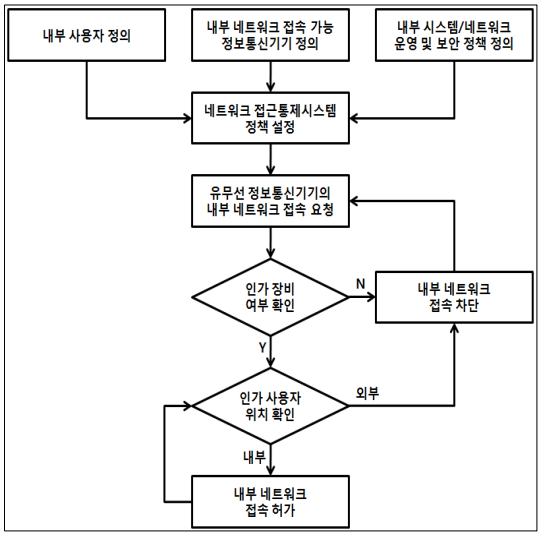


[그림 2] 의료 정보유출 방지를 위한 이중 접근통제 모델

여기서 사용자 정보 획득 인터페이스는 조직 내외로 이동하는 사용자를 식별하는 역할을 수행한다. 이 정보를 바탕으로 기 등록된 사용자 정보와 구축된 인증시스템 환경 정보를 비교하여, 실제 사용자가 조직 내에 위치

하는 지의 여부를 판별한다. 이 결과 값을 네트워크 접근통제 시스템 정책에 반영하여, 내부 네트워크에 접근 허용 또는 차단을 결정한다. 이 과정의 세부 절차는 [그림 3]과 같이 표현된다.

이때 내부 네트워크 접근통제정책은 제안된 모델을 구현하고자 하는 조직의 기존 의료 보안정책과 연계된다. 예를 들어, 인증된 사용자 및 정보통신 디바이스만이 내부 자원을 사용하게 하는 것[1]과 같은 기본 보안정책에 또 다른 인증 절차를 추가하여[14][16], 실제 사용자의 명확한 식별과 필요에 의한 내부 네트워크 접근을 판단할 수 있는 것이다. 따라서, 기존의 내부 규정, 지침 또는 의료 보안정책에 이중 인증을 위한 사용자 준수 사항을 반영하는 것은 의료 정보보호 강화 및 네트워크 이중 접근통제 시스템의 성공적 운영을 위해 필수적이며, 지속적인 사용자 보안인식 교육도 병행해서 추진해야 한다.

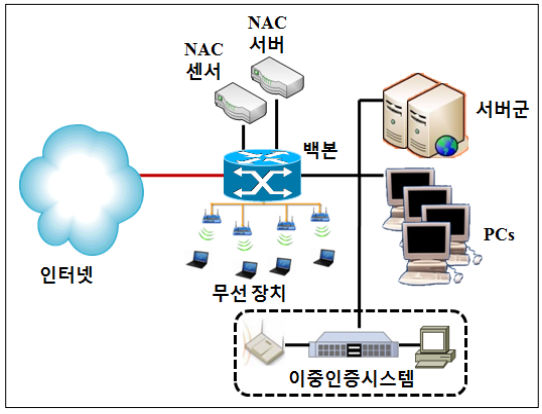


[그림 3] 네트워크 이중 접근통제 실행절차

4. 제안모델 구현 및 평가

4.1 네트워크 이중 접근통제 모델 구현

본 연구에서 제안되는 네트워크 이중 접근통제 모델은 150명의 사용자가 있는 N기관에서 적용되었으며, 시스템 및 네트워크 구조는 하기 [그림 4]와 같다.



[그림 4] 네트워크 이중 접근통제 구조

내부 네트워크에 접근하고자 하는 정보통신 디바이스를 식별하는 NAC(Network Access Control) 센서와 접근통제정책을 수립하고 실행하는 NAC 서버가 네트워크 접근통제 시스템을 구성한다. 이 시스템과 이중인증시스템을 연동하여, 실제 사용자의 조직 내 위치 여부를 기준으로 네트워크 접근통제정책을 실행한다.

4.2 네트워크 이중 접근통제 모델 평가

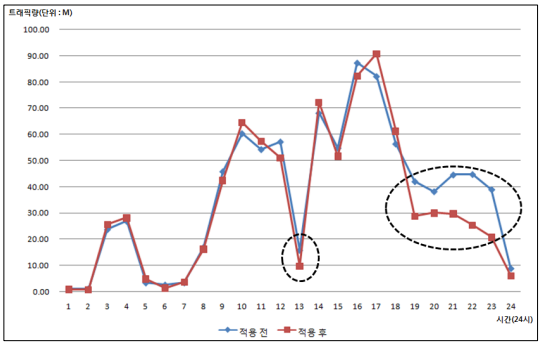
4.2.1 확장성 및 범용성

이중인증 시스템 내 사용자 정보 획득 인터페이스는 다양한 방법을 이용한 사용자 이동 정보 수집이 가능하여, 확장성이 뛰어나다. 본 연구에서는 객체의 이동을 추적 및 관리하기 위해 응용되는 RFID[4][10][17]를 건물 출입통제 시스템에 적용하여 활용하였으나, 특정 지역의 상황정보를 인식할 수 있는 서베일런스 시스템에서도 활용 가능하다. 특히, 소지 또는 존재 기반으로 식별 및 인증을 위해 사용되는 방법은 사용자 이동성을 지식 기반보다 더 강하게 표현하고 있으므로, 이중인증 시스템에 적용하기에 적합하다. 제안된 모델은 다양한 환경에서도 의료 정보 유출을 방지하기 위한 네트워크 접근통제 정책에 적용될 수 있는 확장성과 범용성을 갖추었다.

4.2.2 불필요/유해 트래픽 감소

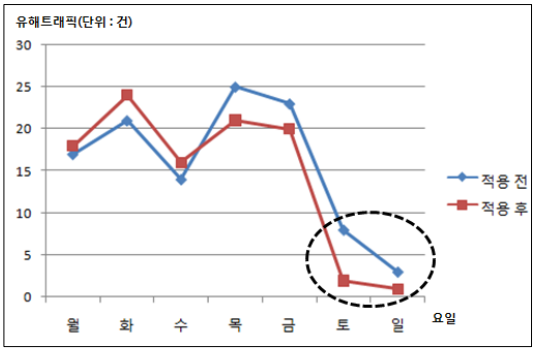
구현된 의료 정보유출 방지를 위한 네트워크 이중 접근통제 모델을 이용한 트래픽 측정은 N기관이 기 보유하고 있던 UTM(Unified Threat Management)과 TMS(Threat Management System)를 이용하여 2주간 진행되었다. 이때, 비교를 위해 이중인증 시스템을 적용하기

전 2주간 데이터를 별도로 데이터베이스에서 추출하였다. 실험 결과, 불필요 트래픽은 [그림 5]에서 볼 수 있는 바와 같이 일 평균 8%가 감소하였다.



[그림 5] 불필요 트래픽 감소량 비교도

이와 같이 트래픽이 감소한 결과는 제안된 모델이 네트워크 자원의 효율적 이용을 가능하게 한다는 의미를 지닌다. 물론 최근 PC에 적용된 윈도우즈 운영체제는 절전모드를 통해 불필요 네트워크 사용을 억제하긴 하나, 제안된 모델은 사용자 부주의 또는 PC 설정 변경으로 인해 사용되는 네트워크 사용량도 통제 가능하기 때문에 안정적으로 의료 보안정책을 집행할 수 있는 장점이 있다. [그림 5]에 원으로 표시된 부분은 사용자의 건물간 이동 시 네트워크 트래픽 량이 확연히 감소한 부분을 보여주고 있다.



[그림 6] 유해 트래픽 감소량 비교도

실험 결과, 유해 트래픽은 상기 [그림 6]에서 볼 수 있는 바와 같이 일 평균 8%가 감소하였다. 이 결과는 제안된 모델이 실제 사용자가 건물 내부에 위치할 때에만 내부 네트워크에 접근을 허가하기 때문에, 사용자 부재 시 인가된 정보통신 디바이스라 할지라도 외부 네트워크에 임의 접속하는 것을 차단하는 것에서 비롯된다. PC 또는 노트북 등이 외부 네트워크에 임의 접속하는 것은 일반적으로 의료 정보 유출형 악성코드 감염으로 발생하며, 사용자가 인지하기 어렵기 때문에 제안된 모델과 같은 의료 보안구조를 도입하여 차단해야 한다. [그림 6]에 원으로 표시된 부분은 사용자가 소수인 주말간 상황이며, 제안된 모델이 효과적으로 네트워크 사용을 통제하고 있는 것을 보여준다.

5. 결론

본 논문에서는 의료 정보유출 방지를 위한 네트워크 이중 접근통제 모델을 제안하였다. 본 연구에서 제안한 네트워크 이중 접근통제 모델은 사용자가 실제 조직 내부에 위치하고 있어 인가된 정보통신 디바이스를 활용하는 때에만 내부 네트워크 접속을 허용한다. 그러므로 비인가자의 내부 네트워크 접근을 차단하고, 허가된 사용자 부재 시의 불필요 외부 인터넷 접속을 차단함으로써 의료 정보를 보호할 수 있는 안전한 환경을 제공한다. 또한 별도의 에이전트를 필요로 하지 않아 사용자 단말기의 개인 프라이버시를 보호할 수 있다.

그러나 의료 정보유출 방지를 위한 사용자 이중인증 시스템과 네트워크 접근통제 시스템간의 연동 과정에서 정책의 설정 및 집행 소요시간이 발생하고, 사용자 미식별 또는 식별 오류가 나타날 수 있는 문제점이 있기에, 이를 해결하기 위한 추가적인 연구가 필요하다.

참 고 문 헌

[1] 김도형 · 유재형 · 이동휘 · 기재석 · 김귀남 (2008). LDAP기반의 산업기술 유출방지에 관한 연구. 정보 · 보안 논문지, 8(4), 21-30.

[2] 김영진 · 권헌영 · 임종인 (2008). U-정보사회에서의 포괄적 네트워크 보안관리 방안. 정보보호학회지, 18(3), 74-80.

[3] 김영진 · 이수연 · 권헌영 · 임종인 (2009). 국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구. 정보보호학회논문지, 19(1), 103-111.

[4] 김의창 · 박명수 (2007). RFID를 활용하여 물류정보

처리를 위한 웹 서비스 기반의 연동 미들웨어 시스템. 디지털정책연구, 5(2), 1-13.
[5] 김진섭 (2010). 「위험관리 기반 침해사고 조기 대응 체계」 구축 사례. 정보보호학회지, 20(6), 73-87.
[6] 김종원・최일준・신현준・오창석 (2009). 접속 에이전트 기반 다단계 인증을 이용한 접근 통제 구성. 정보기술학회논문지, 7(4), 218-225.
[7] 노철우・강경태・이지웅・전재현 (2009). NAC (Network Access Control)을 이용한 컴퓨터 네트워크 보안 플랫폼 구성. 한국콘텐츠학회 2009 춘계 종합학술대회 논문집, 7(1 상), 8-11.
[8] 박원형・양경철・이동휘・김귀남 (2008). 정보 유출 악성코드 분석을 통한 개선된 탐지 규칙 제작 연구. 정보・보안 논문지, 8(4), 1-8.
[9] 변진욱 (2011). 효율적이고 안전한 스마트카드 기반 사용자 인증 시스템 연구. 전자공학회논문지, 48(2, TC편), 105-115
[10] 신화성・한경석 (2008). 식품산업의 효과적인 RFID 시스템 도입 방안에 관한 실증 연구. 디지털정책연구, 6(3), 109-119.
[11] 서종렬 (2010). 스마트 시대의 인터넷과 정보보호 과제. 한국통신학회지(정보와통신), 28(1), 29-35.
[12] 이극・지재원・천현우・이규원 (2011). 하이브리드 클라우드 컴퓨팅 환경에 적합한 인증시스템 설계. 정보・보안 논문지, 11(6), 31-36.
[13] 전인자・정경용・이영호 (2011). 의료자산보호에서 얼굴인식을 위한 가보 웨이블릿 분석. 한국콘텐츠학회논문지, 11(11), 10-18.
[14] 이춘재・조기량 (2007). 네트워크 이중 인증을 통한 역할 기반 개방형 네트워크 접근 통제 시스템의 구현. 한국통신학회논문지, 32(8), 502-508.
[15] 유한나・이재식・김정재・박재표・전문석 (2011). 인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식. 한국통신학회논문지, 36(8), 939-946.
[16] 최경호・김종민・이대성 (2012). RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템. 정보・보안 논문지, 12(3), 53-58.
[17] 하태현 (2009). RFID를 이용한 교과 수준별 이동수업 출석 시스템 개발에 관한 연구. 디지털정책연구, 7(4), 159-168.
[18] Dong Hwi Lee, Kyong ho Choi and Kuinam J. Kim, Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique, Computational Science and its Applications - ICCSA 2007, Lecture Notes in Computer Science, 2007, Volume 4706/2007, pages 181-192.
[19] Lawrence Orans・Mark Nicolett (2005). Gartner's Network Access Control Model. Gartner IT Security Summit 2005.

최 경 호

・2002년 경기대학교 경제학과(학사)
・2005년 경기대학교 경제학과(석사)
・2008년 경기대학교 정보보호학과(박사)
・2012년~현재 경기대학교 산업기술보호특화센터 연구교수
・관심분야 : 보안아키텍처, 인터넷 보안, 정보보호정책관리
・E-mail : cyberckh@gmail.com

강 성 관

・2001년 인하대학교 컴퓨터공학부(학사)
・2005년 인하대학교 정보통신공학과(석사)
・2006년~현재 인하대학교 정보공학과(박사과정)
・관심분야 : 영상처리, 컴퓨터 비전, HCI
・E-mail : kskk1111@empas.com

정 경 용

・2000년 인하대학교 전자계산공학과(학사)
・2002년 인하대학교 컴퓨터정보공학과(석사)
・2005년 인하대학교 컴퓨터정보공학과(박사)
・2006년~현재 상지대학교 컴퓨터정보공학부 교수
・관심분야 : 인터넷 보안, 데이터마이닝, 의료자산보호, HCI
・E-mail : dragonhci@hanmail.net

이 정 현

- 1977년 인하대학교 전자과(학사)
- 1980년 인하대학교 전자공학과(석사)
- 1988년 인하대학교 전자공학과(박사)
- 1979년~1981년 한국전자기술연구소 시스템 연구원
- 1984년~1989년 경기대학교 전자계산학과 교수
- 1989년 ~ 현재 인하대학교 컴퓨터공학부 교수
- 관심분야 : IT융합기술, HCI, USN
- E-mail : jhlee@inha.ac.kr