Journal of The Korea Society of Computer and Information
Vol. 19, No. 10, October 2014

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.10.185

역할기반 응급의료정보보안시스템 REMISS의 설계

김 형 훈*, 조 정 란*

A Design Of Role-based Emergency Medical Information Security System REMISS

Hyung-Hoon Kim *, Jeong-Ran Cho *

요 약

본 논문에서는 기존의 응급의료정보시스템에 정보보안 개념을 도입한 역할기반 응급의료정보보안시스템 REMISS를 설계하였다. 또한 HL7 기반의 응급의료정보 및 보안정보를 위한 메시지 구조와 프로토콜을 제시하였다. REMISS의 보안 절차는 사용자인증단계와 역할/권한배정단계로 이루어져 있다. REMISS는 보안정보를 사용하여 응급의료정보시스템의 각 사용자에게 그 역할에 맞는 권한을 부여하고 허가된 권한 내에서 응급의료정보를 접근하도록 할 수 있으므로 적절한 보안 서비스를 제공할 수 있다. 그리고 응급상황 발생시에 동적으로 보안정보를 교환하여 권한을 부여함으로써 각 사용자의 역할 변경에 대응할 수 있는 이점이 있다.

▸ Keywords : 정보보안시스템, 응급의료정보시스템, 보안시스템, 병원정보시스템, 프로토콜

Abstract

In this paper, we designed a role-based emergency medical information security system REMISS added the security concept to the existing emergency medical information system. Also we suggested a REMISS protocol based on HL7 for using the emergency medical information and the security information. The procedure of security consists of user authentication phase and role/permission assign phase in the REMISS. The REMISS can supply proper security service since the REMISS assign proper permissions to each users of emergency medical information system and allow the user to access the permitted emergency medical information by using security information of the REMISS. There are some advantages that REMISS can adapt to the changing of the role of each user by dynamic exchanging the security information and assigning permissions to each user.

▸ Keywords : Information Security System, Emergency Medical Information System, Security System, Hospital Information System, Protocol

•제1저자 : 김형훈 •제2저자 : 조정란
•투고일 : 2014. 8. 19, 심사일 : 2014. 9. 6, 게재확정일 : 2014. 9. 22.
* 광주여자대학교 보건의료시스템학과(Dept. of Biomedical Systems, Kwangju Womens University)

I. 서 론

정보통신 기술의 지속적인 발전과 최근의 스마트폰으로 대표되는 이동 통신 환경은 사회 전반에 대한 정보화 사회의 절정을 이루는 모습으로 나타나고 있다. 이와 같은 정보화의 가속화는 보건의료 분야에 있어서도 많은 변화를 요구하고 있으며 무선 네트워크와 다양한 모바일 단말기를 활용한 다양한 의료서비스가 시도되고 있다. 의학기술과 정보통신기술의 융합은 환자 중심의 고도화된 양질의 의료서비스를 제공할 수 있는 환경을 만들어 주고 있다. 그러나 환자가 병원에 이송되기 이전의 단계, 즉 응급구조 및 응급처치의 단계가 환자의 건강 및 생명 유지에 있어 매우 중요한 단계이므로 이를 위한 응급의료체계에 많은 관심과 관련 연구가 진행되고 있다.[1]

각 나라마다 서로 다른 사회의료제도나 자연환경에 처해 있으므로 그 나라만의 독특한 응급의료체계가 구축되어 있다. 일반적으로 응급의료체계는 응급환자가 발생하였을 때, 현장에서 적절한 처치를 시행한 후, 신속하고 안전하게 환자를 치료에 적합한 병원으로 이송하고, 병원에서는 응급의료진이 의료기술과 장비를 집중하여 환자를 치료하도록 지원하는 체계를 말한다. 응급의료체계는 일반적으로 병원전단계와 병원단계로 구성되며, 우리나라의 응급의료체계의 흐름은 그림 1과 같다.[2]

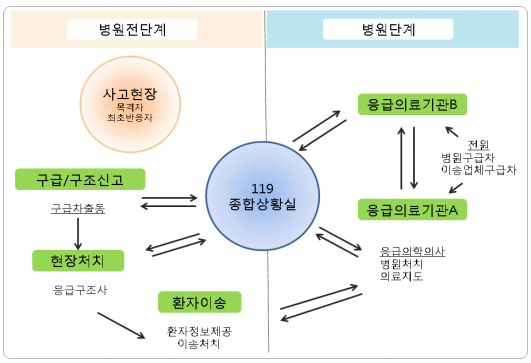

그림 1. 우리나라 응급의료체계의 흐름
Fig. 1. Flow of Emergency Medical Service System in Korea
Sources:National Emergency Medical Center

양질의 응급의료서비스를 제공하기 위해서는 응급의료체계의 각 구성요소와 관리자들을 하나의 완전한 유기체로 만들어 주어야 하며 이에 대한 우리나라의 응급의료정보통신 체계의 모식도는 그림 2와 같다.[2]

이러한 응급의료체계 속에서 응급의료정보시스템은 응급환자에 대해 적절한 전문 응급처치를 할 수 있도록 일반적 응급처치 정보뿐만 아니라 해당 환자에 대한 의료정보를 제공하는 역할을 수행한다. 또한 병원전단계에서 응급환자에 대해 수집한 의료정보를 이송 병원에 시스템을 통해 효율적으로 전달함으로써 병원단계에서 신속하게 환자 치료가 이루어질 수 있도록 역할을 수행해야 한다.[3]

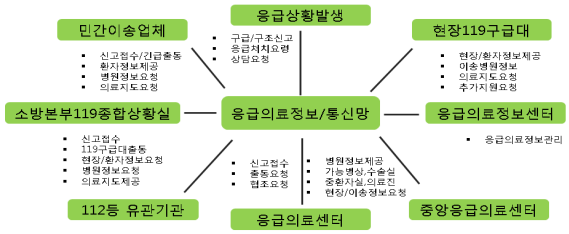

그림 2. 우리나라 응급의료정보통신체계 모식도
Fig. 2. Organization of Emergency Medical Information Service System in Korea
Sources:National Emergency Medical Center

응급의료체계는 응급구조사, 의료진의 여러 역할자가 존재하며, 구급대, 응급의료센터, 진료병의원의 여러 기관이 연계되어 있다.[4] 환자에 대한 의료정보가 응급의료체계 안에서 원활하게 현실적으로 사용되기 위해서는 정보보안의 안전성이 확보되어야 한다. 따라서 다양한 기관 및 사용자가 관여하는 응급의료체계에 적합한 새로운 정보보안 모델이 필요하며, 본 논문에서는 이에 대한 정보보안 모델을 제시하고자 한다. 응급의료체계에 관여된 각 기관 및 시스템은 독자적인 시스템 체계와 정보보안 체계를 갖추고 있다.[5] 따라서 서로 다른 각 기관 및 시스템이 한 응급의료체계 안에서 유기적으로 연계되어 상호간에 응급의료 구조에 필요한 의료정보를 원활하게 교환하기 위해서는 본 논문에서 제안하는 것과 같은 통합된 정보보안 체계가 수립되어 있어야 한다.

보건 및 의료정보 분야에서 서로 다른 정보시스템 사이에 의료정보 공유 및 접속을 위한 메시징과 프로토콜을 제공하는 HL7(Health Level 7)이 산업 표준으로 일반화 되어있다.[6] 본 논문에서는 응급의료체계에 적합한 응급의료정보보안시스템의 체계를 정의하고, 다양한 사용자가 상호 협력하여 운영되는 응급의료체계 환경에 적합한 역할기반 정보보안 시스템을 제안하였다. 또한 응급구조 현장에서 응급구조사에 의한 보다 전문적이고 적극적인 응급처치를 지원하기 위해 응급의료정보, 진료정보, 사용자보안정보의 교환이 필요하며, 이를 위하여 HL7기반의 응급의료정보 프로토콜을 제시하였

다. HL7은 일반적인 의료정보만을 위한 것이기 때문에 응급의료정보 및 보안정보를 위한 메시지 구조 및 프로토콜을 설계하였다.

본 논문의 구성은 다음과 같다. 2장에서는 응급의료정보시스템의 개념과 기존의 존재하는 시스템의 주요 특징을 살피고, 보건의료정보시스템의 상호 의료정보 교환에 필요한 프로토콜의 개념과 의료정보의 보안에 대한 개념과 특징을 기술하였다. 3장에서는 다양한 기관 및 사용자가 존재하는 응급의료체계에서 효율적인 정보보안시스템의 모델을 제안하였고 4장에서 결론을 기술하였다.

II. 이론적 배경

1. 응급의료정보시스템의 개념

현대의 의료서비스는 기존의 의학기술이 첨단 의료기기시스템, 생명공학기술, 정보통신기술과 접목되어 높은 수준의 의료서비스로 제공되고 있다. 이와 같은 높은 수준의 의료서비스는 환자가 병의료기관에 적절한 시점에 진료 및 치료를 받을 때 의미 있는 상황이다. 특히, 사회구조가 복잡해지면서 여러 가지 대형 재난이 발생될 가능성도 높아져 가고 있다. 또한 전 세계적으로 고령화 사회로 변화해 가고 있으며 고령자의 비율이 높아진 만큼 이들의 만성질환성 응급상황 등을 고려해 볼 때 전체적인 응급상황 발생 가능성이 높아졌다고 볼 수 있다. 이것은 앞으로 환자에게 제공될 높은 수준의 의료서비스의 결과를 만들어내기 위해서는 병원 도착 전 응급의료체계의 역할이 매우 중요하다는 것을 의미한다.

응급의료정보시스템은 응급구조사가 응급상황이 발생되었을 때 실시간으로 발생된 상황에 가장 적합한 응급처치를 수행할 수 있도록 하기 위한 시스템이다. 환자에 대한 적합한 응급처치는 응급환자에 대한 정확하고 신속한 응급의료정보의 파악 및 평가가 요구된다. 환자에 대한 응급의료정보가 부재한 상황에서의 응급처치는 불가능하며, 오히려 더욱더 위급한 상황을 만들 수 있다. 응급의료정보시스템은 응급환자에 대해 당뇨병력, 협압, 알레르기, 천식 등 기존 병력에 대한 정보를 제공하여 적극적인 구조 활동을 가능하게 해준다.[6] 응급처치에 대한 경험적 지식을 환자의 병이력정보와 함께 체계적으로 지식데이터베이스에 관리, 운영함으로써 더욱더 적합한 응급처치와 병원인계가 이루어지도록 이에 대한 연구가 계속되고 있다.

응급의료정보통신체계에서 정보통신망의 근간이 되는 백본 통신망은 유선을 많이 이용하고 있으며, 단말 사용자 측에서는 이동 통신기술의 발달과 모바일 서비스의 편리성 때문에 PDA, 스마트폰과 같은 모바일 단말기를 이용할 수 있는 무선통신이 일반화되고 있다. 스마트폰과 같은 모바일 단말기를 사용하여 응급의료체계를 사용할 수 있는 시스템으로 대표적인 것이 보건복지부의 실시간 응급의료 정보제공 시스템이다. 제공되는 주요 기능은 및 정보는 실시간 응급의료기관 검색, 응급기관(119) 연결, 자동심장충격기 위치정보, 증상별 응급처치 요령, 독극물 정보 등이 있다. 그러나 보건복지부 실시간 응급의료정보시스템은 응급정보의 접근성과 환자 및 응급상황에 대한 정보가 부족하여 적극적인 응급구조체계 활용에 한계점을 가지고 있다.

경험적 지식을 활용한 응급의료정보시스템 설계의 연구에서는 보건복지부 실시간 응급의료 정보제공 시스템을 개선하기 위해 기존 시스템을 접목하여 제공되는 서비스를 활용하면서 병원전단계에 최초반응자와 응급구조사가 응급환자에 대해 응급처치함에 있어 이를 지원할 수 있는 경험적 지식기반 응급의료정보를 제공하고 있다. 경험적 지식기반 응급의료정보시스템은 사용자를 일반사용자, 응급구조사, 병원의원사용자로 구분하고, 로그인 과정 이후 해당 사용자에 맞는 전용서비스를 사용할 수 있도록 하고 있다. 특히 응급의료지식데이터베이스는 응급처치에 대한 경험적 지식을 체계화하여 저장, 검색 서비스를 제공하여 응급상황에 효과적으로 사용될 수 있도록 한다. 또한 등록된 환자에 대한 병원진료 정보를 제공함으로써 보다 적극적인 응급처치를 수행할 수 있도록 하고 있다.[7]

보다 발전된 보건의료서비스를 제공하기 위해 병원단계의 진료서비스뿐만 아니라 응급환자의 정확하고 신속한 응급처치와 병원인계 과정인 병원전단계의 과정이 매우 중요한 단계로 주목을 받고 있으며, 이를 위해 응급의료정보시스템에서 환자에 대한 정확한 응급의료정보 및 진료정보의 제공을 통해 보다 전문적인 응급처치를 위한 연구들이 계속되고 있다.

2. 의료정보시스템의 프로토콜

컴퓨터통신기술 및 정보처리기술의 발달이 사회 각 분야의 정보화를 가능하게 했고, 그 가운데 의료정보화는 의료서비스를 개선하여 보다 높은 수준의 양질의 서비스를 제공하기 위하여 활발히 진행되어 왔다. 그러나 의료정보화가 각 병의원, 각 부문마다 서로 다른 규격과 환경으로 구축되어 운영됨으로 인하여 서로 다른 병원에서 뿐만 아니라 한 병원 내에서도 이질적인 의료정보시스템들이 존재하게 되었다. 이로 인하여 한 병원 전체적인 입장에서 의료서비스의 생산성 및 의료정보의

재사용성이 매우 떨어지고 있다. 또한 환자의 입장에서 의료정보의 병원간 원활한 교환이 어려운 상황으로 인하여 타 병원에서 이미 검사 및 진료 받은 내용을 불필요하게 중복하여 재검사 및 진료를 받아야 하는 불편을 겪게 된다.

HL7은 서로 다른 보건의료분야 소프트웨어 애플리케이션 간에 정보가 호환될 수 있도록 하는 사실상 보건의료 산업계의 표준 프로토콜이다. HL7은 의료기관의 유형 또는 규모에 상관없이 모든 종류의 의료업무(patient management, laboratories, pharmacies, system management 등)의 서비스 요구수준을 충족시킬 수 있다. HL7은 보건의료분야 관계자의 요구와 변화를 수용하는 새로운 버전으로 업그레이드되어 가고 있으며 각 나라의 언어와 요구사항을 수용한 국제적 표준으로 발전되어 가고 있다.

HL7은 ISO의 OSI 7계층 참조모델의 7번째 계층인 응용계층 프로토콜에 해당되는 부분을 다루고 있다. HL7에서는 메시지구조(abstract message definition), 코딩규칙(encoding rules), 트리거이벤트(trigger events) 세 가지를 대상으로 명세화하고 있다. 메시지는 크게 트리거이벤트(trigger events), 쿼리(query), 확인응답(acknowledgement)으로 구성된다. 트리거이벤트로 인한 ADT(Admission, Discharge and Transfer) 메시지가 발생하면 쿼리 메시지로 전달되고 응답시스템은 잘 처리되었다는 확인응답을 하게 된다.[8]

HL7 메시지는 표 1, 표 2와 같이 메시지헤드(MSH: Message Header), 이벤트타입(EVN:Event Type), 환자아이디(PID:Patient Identification) 세그먼트들로 구성된다.

표 1. ADT 메시지
Table 1. ADT Message

세그먼트	세그먼트 설명
MSH	Message Header
EVN	Event Type
PID	Patient Identificatoin

표 2. ACK 메시지
Table 2. ACK Message

세그먼트	세그먼트 설명
MSH	Message Header
MSA	Message Acknowledgement
[ERR]	Error

각 세그먼트는 데이터필드(data field)와 컴포넌트(component) 단위로 세분된다. 트리거이벤트의 이벤트 타입은 표 3과 같다.

표 3. 이벤트타입
Table 3. Event Type

이벤트	이벤트 설명
A01	ADT/ACK - Admit/visit notification
A02	ADT/ACK - Transfer a patient
A03	ADT/ACK - Discharge/end visit
A04	ADT/ACK - Register a patient
A05	ADT/ACK - Pre-admit a patient
…	…

3. 의료정보 보안의 개념

컴퓨터통신기술 및 정보처리기술의 의료분야에 대한 적용 및 개발은 계속하여 확장될 전망이며 이러한 의료정보화는 일반적인 병의료분야의 행정적인 정보뿐만 아니라 환자의 진료정보까지 확산되어 사용되고 있다. 정보처리시스템에 다루어지는 일반적인 정보도 철저한 정보보안이 밑바탕이 되었을 때 현장과 실무에 사용 가능한 것이며, 환자에 관한 의료정보는 사생활 침해 등 매우 민감한 정보로써 더욱더 철저한 정보보안이 이루어지지 않고서는 컴퓨터를 이용한 정보화가 불가능한 내용이다. 의료정보의 노출은 개인에게 돌이킬 수 없는 정신적, 사회적, 경제적 피해를 초래할 수 있어 중요하게 다뤄져야한다. 사적비밀보장과 의료정보보안은 환자와 의사간의 신뢰관계를 형성시키며 효과적인 의료행위를 가능하게 하는 기본적인 환경이라 할 수 있다.[9]

최근의 정보통신 이용 환경이 무선 네트워크와 모바일 단말기를 사용하는 환경으로 발전해 가고 있으며, 병원정보시스템 환경 또한 이와 같은 변화가 일어나고 있다. 본 논문에서 관심을 두고 있는 응급의료정보통신체계는 현장 이동성 및 편리성으로 인해 이와 같은 무선 통신 환경이 더욱더 요구되는 환경이다. 무선통신망환경은 정보보안 측면에 있어서는 유선통신망 환경에 비해 더욱더 취약한 환경으로 이에 적합한 보안대책이 요구되어 진다. 무선통신망과 공중망을 거쳐 의료정보를 상호 교환하기 위해서는 불순한 의도를 가진 공격자에 의해 중간에 가로챌 수 있다는 것을 고려하여 암호화 시스템을 사용한다. 암호화시스템은 암호화와 복호화에 서로 다른 키를 사용하여 키 전송이 필요 없으며 디지털 서명이 가능한 공개키암호화방식과 암호화 키와 복호화 키가 동일하여 송수신자 간에 비밀키를 공유하는 비밀키암호화방식이 있다.

정보보안은 비밀성(security), 무결성(integrity), 가용성(availability)의 보안 요구 조건이 만족되어야 한다. 비밀성은 오직 인가 받은 사용자만이 접근될 수 있음을 보장해야 함을 말한다. 무결성은 오직 인가 받은 사용자만이 정보를 수정할 수 있도록 보장하여 사실과 다르거나 부정확한 정보가

저장되지 않도록 보장하는 것을 의미한다. 가용성이란 오직 인가 받은 사용자만이 사용할 수 있어야 하며, 인가 받은 사용자는 언제나 사용 가능해야 함을 보장하는 것을 의미한다.[10, 11]

환자의 사생활 보장과 진료기록의 비밀보장을 위해 의료정보의 조작자는 정보에 대한 접근과 사용 권한이 조정되고 관리될 필요가 있다. 사용자의 종류, 자료의 종류, 자원의 종류, 접근종류에 대한 합법적인 접근의 명백한 정의를 포함한 정보보안 정책을 수립해야 한다. 의료 분야에서 사용자의 종류는 의사, 간호사, 사무직 등으로 분류하여 각 사용자의 역할에 합당한 접근 권한을 부여해야 하며, 자료의 종류는 인구학적 자료, 예방접종 등의 일반적인 비기밀사내용과 질병과 관련된 민감한 정보 그리고 정신과 진료내용, 약물 중독 자료 등과 같은 극비사항으로 분류되어 접근이 통제되어야 한다.[12]

의료정보와 같이 다수의 사용자가 다수의 정보를 공유하는 정보통신 환경에서는 어떤 사용자가 어떤 정보에 접근(읽기, 쓰기, 변경)하는 것을 허용할 것인가를 결정하는 접근제어 방법이 중요한 보안 문제의 하나로 다루어지고 있다. 이러한 문제를 다루기 위해 여러 가지 접근 제어 모델이 연구되어 있는데, 접근제어 리스트(ACL: Access Control List) 모델, 강제적 접근제어(MAC: Mandatory Access Control) 모델, 임의적 접근제어(DAC: Discretionary Access Control) 모델, 역할기반 접근제어(RBAC: Role-Based Access Control) 모델이 대표적이다.[2] 본 논문에서 적용하고 있는 역할기반 접근제어는 임무분리(separation of duty) 정책의 보안 원리를 부여해야 한다. 임무분리 정책은 사용자들의 권한 남용이나 오용에 의한 사기, 공모를 방지하기 위하여 민감한 권한들은 한 사람에게 부여하지 않고 여러 사람에게 분산하여 부여해야 한다는 보안 원리이다.

임무분리의 종류에는 정적임무분리(static separation of duty), 동적임무분리(dynamic separation of duty), 연산상의임무분리(operational separation of duty)가 있다. 정적임무분리는 사용자에게 임무분리 관계에 있는 두 개 이상의 역할을 동시에 부여할 수 없다는 정책을 말한다. 동적임무분리는 사용자에게 임무분리 관계에 있는 두 개 이상의 역할을 동시에 부여할 수 있지만 동시에 활성화하여 사용할 수 없도록 하는 정책이다. 연산상의임무분리는 어떤 작업이 여러 단계의 연산으로 구성되어 있다고 했을 때 한 사용자가 모든 단계의 연산을 수행하지 못하도록 하는 정책이다. 본 논문에서는 권한 관리의 유연성을 가지며 응급의료체계 환경에 적합한 동적임무분리 정책을 기반으로 기술하였다.

III. REMISS 설계

1. REMISS 구조

본 논문에서 제안한 역할기반 응급의료정보보안시스템(REMISS:Role-Based Emergency Medical Information Security System)의 응급의료정보 보안체계 구성도는 그림 3과 같이 응급의료정보시스템, 응급의료정보보안시스템, 응급구조클라이언트, 일반사용자클라이언트, 병의원클라이언트로 구성된다.

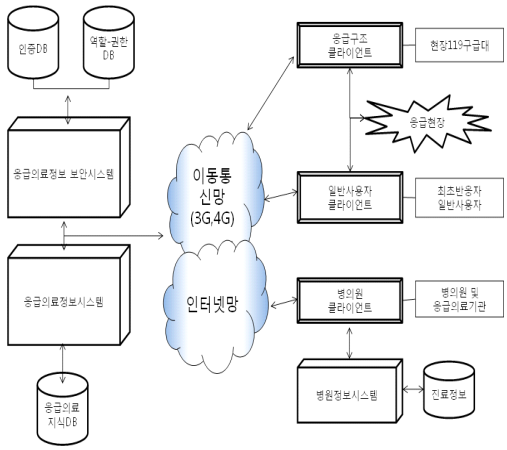

그림 3. 역할기반 응급의료정보보안시스템 구성도
Fig. 3. Organization of Role-based Emergency Medical Information Security System REMISS

응급의료정보시스템은 사용자를 일반사용자, 응급구조사, 병의원사용자로 구분하여 해당 사용자의 역할과 권한에 맞는 서비스를 제공한다. 각 사용자는 응급의료정보시스템을 사용하기 위해 명시된 절차와 양식에 맞추어 개인인증정보를 사용하여 등록하게 되며 이에 대한 처리는 응급의료정보보안시스템(REMISS)에 의해 관리된다. REMISS은 각 사용자에 대한 인증정보뿐만 아니라 응급의료정보 접근 및 이용에 대한 사용자 역할별 접근권한을 관리한다. 응급의료정보시스템은 병의원사용자 클라이언트를 통하여 연계하여 운영될 응급의료센터와 병의원에 대한 정보를 응급의료지식데이터베이스에 등록하고 온라인으로 최신의 정보를 유지함으로써 응급구조 상황에 실시간으로 활용될 수 있도록 운영된다.

응급의료지식데이터베이스는 응급의료정보시스템에 접수된 응급처치 사례에 대한 경험적 지식을 체계화하여 저장하여

응급구조 현장 상황에 효과적이며 신속한 응급처치가 이루어질 수 있도록 활용된다. 이때 응급구조사는 REMISS로부터 인가된 접근권한을 사용하여 응급의료지식데이터베이스와 연계된 응급의료센터 및 병의원에서 제공되는 응급의료정보를 활용하여 환자에 대해 적극적인 응급구조 활동을 수행하게 된다.

모든 응급의료정보는 응급의료정보시스템을 통하여 관련 기관 및 사용자에게 전달되도록 한다. 응급의료정보시스템은 응급의료정보보안시스템과 연계하여 사용자 인증, 의료정보 접근제어의 정보보안 체계를 통하여 응급의료정보 서비스를 사용자에게 제공하는 역할을 수행한다. 응급의료정보시스템과 응급센터 및 병의원 기관의 정보시스템 사이의 응급의료정보 및 인증정보는 본 논문에서 설계한 HL7 기반의 REMISS 프로토콜(3.3절 참조)을 통하여 상호 교환한다.

본 논문에서 설계한 응급의료 보안체계의 응급의료정보의 제공 처리 절차 및 인증 절차는 다음과 같다. ①응급현장에서 119종합상황실을 통하여 구급 및 구조신고를 접수한다. ② 119종합상황실은 신고 접수된 내용을 기반으로 현장에 119 구급대를 출동시키며, 응급구조사에 대한 역할 및 권한 부여와 함께 신고 접수된 내용을 전달한다. ③응급구조사는 응급현장에서 현장상황 및 응급환자의 생체정보를 취득하고 응급처치 정보를 요청한다. ④응급의료정보시스템은 저장된 응급처치정보를 응급구조사에게 전달하고 응급의료기관 및 응급의료지도 의사의 역할 및 권한을 부여한다. ⑤응급구조사와 응급의료지도 의사가 상호간에 응급처치, 진료정보, 환자생체정보를 공유하며 응급구조 활동을 진행하며 응급센터로 환자를 이송한다.

2. REMISS 역할기반 접근제어

2.1 REMISS 인증 알고리즘

REMISS는 사용자 인증과 사용자 역할기반 접근제어 매커니즘을 통하여 응급의료정보 보안 체계를 구성한다. 이를 위하여 REMISS는 사용자인증 데이터베이스와 사용자역할 데이터베이스의 두 가지 보안정보를 관리한다. 사용자인증 데이터베이스는 응급의료정보시스템을 사용하기 위하여 사용자 개인 인증을 위한 정보를 입력받아 사용자 로그인 과정에서 본인 인증을 위한 사용자 인증정보를 저장한다. 사용자역할데이터베이스는 응급의료정보체계의 사용자 유형과 각 사용자 유형에 대한 역할 및 권한을 정의하며 사용자 인증과정이 확인된 사용자에게 역할 및 권한을 배정하기 위한 역할 및 권한 정보를 저장한다. REMISS의 인증 알고리즘은 사용자인증단계와 역할 및 권한배정단계의 두 단계로 구성되며 이의 흐름도는 그림 4와 같다.

REMISS 인증단계의 첫 번째 단계인 사용자인증단계는 정적인 사용자 인증정보를 확인하는 과정으로써 이 단계를 거치면 응급의료정보시스템에 대한 일반적인 서비스를 사용할 수 있다.

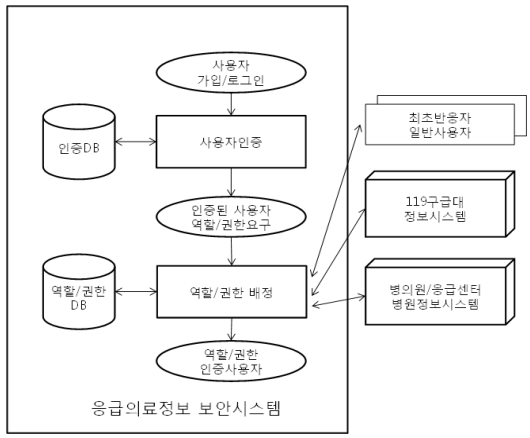

그림 4. REMISS 인증 및 역할배정 알고리즘의 흐름도
Fig. 4. Flow of REMISS Authentication and Role/Permission Assign Algorithm

REMISS 인증단계의 두 번째 단계인 역할/권한배정단계는 응급구조 상황 발생시에 사용자인증단계를 거친 사용자에 대하여 동적으로 그 역할과 권한을 배정하는 단계이다. 사용자인증과정에서 확인된 사용자의 소속 기관의 정보시스템에게 REMISS 프로토콜의 보안메세지를 통해 해당 사용자의 사용자 역할 및 권한 부여에 필요한 정보를 요청하여 역할과 권한을 배정하고 응급의료정보시스템의 서비스를 이용할 수 있도록 한다.

2.2 REMISS 역할/권한 배정

REMISS는 응급의료체계에 존재하는 사용자 역할을 최초반응자, 일반사용자, 응급구조사, 의료지도사로 분류하였다. 역할/권한데이타베이스에 각 사용자 역할에 대한 응급의료정보의 접근권한이 정의되어 있다. 사용자 역할 UserRole의 정의 내용은 다음과 같다.

UserRole = {사용자 | 응급구조팀}
사용자 = {구조사 | 의료인 | 일반사용자 | 관리자}
응급구조팀 = {최초반응자 | 응급구조사 | 의료지도사}

사용자역할의 정의는 클래스의 계층구조로 정의되어 있으

며, 최상위 클래스는 응급의료정보시스템의 일반적인 서비스를 이용하기 위한 '사용자'와 응급구조 활동을 위해 응급구조팀에 배정되어 정해진 역할을 수행하기 위한 '응급구조팀'으로 구성된다. '사용자'의 하위클래스는 다시 '구조사', '의료인', '일반사용자', '관리자' 등으로 구성되어 상위클래스의 속성을 기본으로 하며 각 하위클래스의 추가적 속성으로 정의된다. 이들 사용자역할 클래스들 간의 정보보호의 임무분리를 고려한 계층 구조는 그림 5와 같다.

각 사용자 역할 UserRole-i에 대한 접근권한의 정의 내용은 다음과 같다.

UserPrivilege = {UserRole-i, EmgTarget,
{Operation}, Constraint}

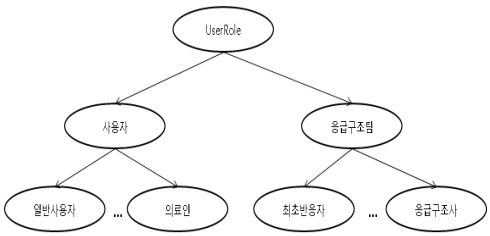

그림 5. 사용자역할 UserRole 계층구조
Fig. 5. Hierarchy of UserRole

각 사용자 역할에 대해 응급의료정보 또는 기능(EmgTarget)에 대한 접근권한(Operation)은 주어진 제약조건(Constraint)을 만족하는 상황에서 사용할 수 있도록 정의되어 있다.

REMISS의 사용자인증단계, 역할/권한배정단계의 두 가지 인증단계를 거친 후 인증된 사용자에 대한 접근제어리스트 AccessList의 정의 내용은 다음과 같다.

AccessList = {UID, UserRole-i, EMGID-i}

인증된 사용자(UID)는 정의된 사용자 역할(UserRole-i)에 대한 제약조건을 만족하고, 소속기관의 사용자 보안정보 메시지 교환을 통하여 해당 응급상황(EMGID-i)에 대한 응급의료정보 및 응급의료체계에 대한 역할 및 접근권한을 갖게 된다.

REMISS의 역할/권한 배정 방법은 인증된 사용자에게 동적으로 부여된다. 응급구조 상황이 발생되었을 때 역할 배정에 대한 인증을 거쳐 권한을 가지게 되며 응급구조 상황이 종료되면 그 역할 및 권한은 상실된다. 그러나 한 사용자가 주어진 환경에 따라 여러 역할을 수행해야 하는 경우가 있을 수 있다. 이를 위하여 정보보호의 임무분리 원칙에 따라 활성화되는 시간을 구분하여 배정함으로써 정보보호의 임무분리 원칙을 따르면서 여러 역할을 수행할 수 있도록 하였다. 응급의료체계는 한 조직체계와 달리 다양한 기관 및 사용자가 존재하고 있어서 사용자의 역할이 수시로 변경될 수 있는 환경이다. 따라서 이와 같은 응급의료체계에는 정적인 역할/권한 배정보다 동적인 역할/권한 배정이 더욱더 적합하고 보안정보관리 차원에서도 보다 효율적인 방법이라 할 수 있다.

2.3 REMISS 프로토콜

응급의료체계에 포함된 응급의료정보시스템과 병의료기관 및 응급센터의 병원정보시스템 그리고 119구급기관의 정보시스템 사이에 적법한 보안 절차를 통한 응급의료정보 교환을 위해 REMISS 프로토콜을 설계하였고 이것은 기본적으로 의료정보 교환의 산업 표준으로 사용되고 있는 HL7을 기반으로 하고 있다. REMISS 프로토콜은 진료정보메시지, 응급의료메세지, 사용자보안정보메시지로 구성되어 있다.

진료정보메시지는 응급환자가 기존에 진료 받았던 병의료기관 및 응급센터에 기록되어 있는 진료정보를 응급구조에 활용하기 위하여 응급의료정보시스템으로부터 요구되어 전달되는 메시지이다. 응급의료메시지는 응급구조현장에서 발생되는 환자생체정보 및 응급처치정보를 병의료기관 및 응급센터 도착 이후 치료 또는 응급구조 활동을 위한 목적으로 응급의료정보시스템을 통하여 병의료기관 정보시스템에 전달되는 메시지이다. 사용자보안정보메시지는 사용자 역할/권한 배정을 위해 인증된 사용자에 대한 정보를 기반으로 사용자의 소속 기관과 REMISS 사이에 교환되는 보안정보 메시지이다.

2.3.1 진료정보메시지 PCIMSG

진료정보메시지는 응급의료정보시스템과 병의료기관 및 응급센터 병원정보시스템 사이에 교환되는 응급환자에 대한 진료정보를 담은 메시지를 의미하며, PCIMSG(Patient Clinic Information Message)로 정의하였다. PCIMSG의 메시지의 문법적 구조는 표 4와 같다. 응급환자에 대한 진료정보를 환자가 기존에 진료 받았던 병원으로 요청할 때에 PCIMSG 메시지를 사용하여 요청하고 정보를 받는다.

표 4. PCIMSG 메시지 세그먼트
Table 4 PCIMSG Message Segment

세그먼트	세그먼트 설명
MSH	Message Header
EVN	Event Type
EMGID	Emergency Identification
PID	Patient Identification
{PCI}	Patient Clinic Information

PCIMSG 메시지는 표 5에 설명되어 있는 각 이벤트를 사용한다.

표 5. PCIMSG 이벤트 타입
Table 5. PCIMSG Event Type

이벤트	이벤트 설명
PCIEVN01	등록 환자 사실 확인 요청
PCIEVN02	등록 환자 사실 응답
PCIEVN03	진료정보 요청
PCIEVN04	진료정보 응답

응급상황 기초정보 EMGID와 응급환자에 대한 기초정보 PID를 사용하여 등록된 병원에 등록 환자 여부를 이벤트타입 PCIEVN01(등록확인요청), PCIEVN02(등록확인응답)을 사용하여 확인하고, 진료정보가 필요한 병원에 진단 및 치료정보를 이벤트 타입 PCIEVN03(요청), PCIEVN04(응답)을 각각 사용하여 요청하고 받는다. 이벤트타입이 요청(PCIEVN01, PCIEVN03)인 경우에는 진료정보 세그먼트 PCI에 요청 받고자하는 진료정보 필드를 명시하여 해당 진료정보를 받을 수 있도록 하였다.

2.3.2 응급의료메시지 EMIMSG

응급구조 현장에서 수집된 환자의 생체정보, 응급처치 등 응급의료정보는 응급의료정보시스템에 기록되고 응급구조 상황에 활용된다. 응급의료메시지는 응급구조 현장의 의료지도 또는 환자 이송 후 신속한 치료를 수행하기 위해 응급의료정보시스템과 병의료기관 및 응급센터 병원정보시스템 사이에 교환되는 응급의료정보를 담은 메시지를 의미하며, EMIMSG(Emergency Medical Information Message)로 정의하였다. EMIMSG 메시지의 문법적 구조는 표 6과 같다.

EMIMSG 메시지는 응급구조 현장에서 응급환자에 대한 혈압, 체온 등 생체정보를 교환하거나 응급처치 정보를 교환하기 위해 사용된다. EMIMSG의 이벤트타입은 표 7과 같다.

표 6. EMIMSG 메시지 세그먼트
Table 6. EMIMSG Message Segment

세그먼트	세그먼트 설명
MSH	Message Header
EVN	Event Type
EMGID	Emergency Identification
PID	Patient Identification
{EMI}	Emergency Medical Information

표 7. EMIMSG 이벤트 타입
Table 7. EMIMSG Event Type

이벤트	이벤트 설명
EMIEVN01	응급 환자 사실 확인 요청
EMIEVN02	응급 환자 사실 응답
EMIEVN03	응급의료정보 요청
EMIEVN04	응급의료정보 응답

응급상황 기초정보 EMGID와 응급환자에 대한 기초정보 PID를 사용하여 응급환자 사실을 EMIEVN01(응급환자 사실 확인요청), EMIEVN02(응급 환자 사실 확인응답)을 사용하여 확인하고, 응급의료정보가 필요한 병원과 이벤트 타입 EMIEVN03(요청), EMIEVN04(응답)을 각각 사용하여 요청하고 받는다. 이벤트타입이 요청(EMIEVN03, EMIEVN04)인 경우에는 응급의료정보 세그먼트 EMI에 요청 받고자하는 응급의료정보 필드를 명시하여 해당 응급의료정보를 받을 수 있도록 하였다.

2.3.3 사용자보안정보메시지 USIMSG

응급의료체계에서는 다양한 기관 및 사용자가 적절한 권한으로 상호 협력하여 응급구조 활동을 수행하는 환경이다. REMISS는 첫 번째 단계인 사용자인증단계를 거쳐 사용자 본인을 인증 확인하고, 두 번째 단계인 역할 및 권한 배정단계를 통하여 발생된 응급상황에 요구되는 사용자에게 역할과 권한을 배정하게 된다. 사용자보안정보메시지는 REMISS가 사용자의 소속 기관과 사용자의 역할에 대한 보안정보를 교환하는 메시지를 의미하며, USIMSG(User Security Information Message)로 정의하였다. USIMSG의 문법적 구조는 표 8과 같다.

응급상황 기초정보 EMGID와 사용자에 대한 기초정보 UID, 사용자 보안정보 USI를 사용하여 사용자 등록 사실을 USIEVN01(사용자 등록 사실 요청), USIEVN02(사용자 등록 사실 응답)을 사용하여 확인하고, 사용자 보안정보가 필요한 병원 또는 응급구조 기관과 이벤트타입 USIEVN03(요청), USIEVN04(응답)을 각각 사용하여 요청하고 받는다.

표 8. USIMSG 메시지 세그먼트
Table 8. USIMSG Message Segment

세그먼트	세그먼트 설명
MSH	Message Header
EVN	Event Type
EMGID	Emergency Identification
UID	User Identification
{USI}	User Security Information

USIMSG의 이벤트타입은 표 9와 같다.

표 9. EMIMSG 이벤트 타입
Table 9. EMIMSG Event Type

이벤트	이벤트 설명
USIIEVN01	사용자 등록 사실 요청
USIEVN02	사용자 등록 사실 응답
USIEVN03	사용자 보안정보 요청
USIEVN04	사용자 보안정보 응답

본 논문에서 제안한 REMISS 프로토콜에 의해 응급의료정보시스템에 보안성을 제공할 수 있는 근거는 각 사용자에 대한 인증과 함께 사용자 그룹별로 허가된 권한만을 사용하여 의료정보를 이용할 수 있도록 REMISS에 의해 관리함으로써 응급의료정보에 대한 비밀성, 무결성, 가용성을 보장하게 된다는 것이다.

IV. 결 론

의학기술의 발전과 함께 정보통신 기술의 융합은 환자 중심의 고도화된 양질의 의료서비스를 제공하는 발전된 의료 환경을 만들어가고 있다. 응급의료체계는 병원전단계에서 응급환자에 대하여 현장에서 환자에게 가장 적합한 응급처치를 수행하고 치료를 위한 병원으로 인계하는 역할을 한다. 환자에 대한 적절하고 적극적인 응급처치는 환자에 대한 응급의료정보 및 진료정보 등 의료정보의 파악 및 평가를 통하여 이루어지며, 응급구조사, 응급의료지도의사, 응급구급기관, 병의원, 응급센터 등 다양한 사용자 및 기관의 협력이 필요하다. 환자에 대한 의료정보가 응급의료체계 안에서 원활하게 현실적으로 사용되기 위해서는 정보보안의 안전성이 확보되어야 한다. 그러나 응급의료체계에 관여된 각 기관 및 정보시스템은 각기 독자적인 정보보안 체계를 갖추고 있어 환자의 의료정보 교환이 어려운 상황이다.

본 논문에서는 응급의료체계에 적합한 응급의료정보보안시스템의 체계를 정의하고, 다양한 사용자가 상호 협력하여 운영되는 응급의료체계 환경에 적합한 역할기반 정보보안시스템을 제안하였다. 또한 응급구조 현장에서 응급구조사에 의한 보다 전문적이고 적극적인 응급처치를 지원하기 위해 응급의료정보, 진료정보, 사용자보안정보의 교환이 필요하며, 이를 위하여 HL7기반의 응급의료정보 프로토콜을 제시하였다. HL7은 일반적인 의료정보만을 위한 것이기 때문에 응급의료정보 및 보안정보를 위한 메시지 구조 및 프로토콜을 설계하였다.

본 논문에서 제안한 역할기반 응급의료정보보안시스템 REMISS는 사용자인증단계와 역할/권한배정단계의 두 단계로 구성되어 운영된다. 역할/권한배정단계는 인증된 사용자의 소속 기관인 응급센터, 병의료기관 등 정보시스템과 REMISS 프로토콜을 통하여 상호 보안정보를 요청, 확인하여 역할과 권한을 배정한다. REMISS의 인증과정을 통하여 인증된 사용자는 응급구조클라이언트, 병의원클라이언트, 일반사용자클라이언트 등 해당 사용자에 대한 응급의료정보시스템의 서비스를 사용하여 적극적인 응급구조 활동에 참여하게 된다. 또한 응급구조 환경에서 REMISS 프로토콜을 사용하여 응급의료정보시스템과 연계 병의료기관의 정보시스템 사이에 응급의료정보메시지, 진료정보메시지를 상호 교환하여 환자의 응급처치 및 치료에 필요한 정확한 의료정보를 제공할 수 있게 된다.

본 논문에서 제안한 역할기반 응급의료정보 보안시스템은 보다 높은 수준의 의료서비스를 제공하기 위하여 연구되고 진행 중에 있는 원격의료 환경에서도 매우 필요한 개념이라 할 수 있다. 원격의료서비스의 환경 또한 정보통신망을 통하여 다양한 사용자 및 기관 사이에 의료정보의 상호 통신을 기반으로 하고 있기 때문에 이를 실현하기 위해서는 본 논문의 의료정보보안의 개념이 반드시 필요하며 이에 활용될 수 있을 것으로 기대된다.

본 논문의 연구범위는 응급의료정보보안시스템의 기본 설계로 한정되어 있으나 이의 실질적 구현을 위해서는 응급의료정보의 표준화, 원격의료의 법적, 제도적 근거의 마련이 필요하다. 또한 유비쿼터스 기술 등 최근 기술 동향을 고려한 보다 편리하고 새로운 응급의료정보시스템의 서비스와 보안서비스에 대한 연구가 필요하다.

참고문헌

[1] H. J. Park, "Implementation of the Smart Emergency Medical System", The Journal of Korea Navigation Institute Vol. 15, No. 4,

pp.646-654, Aug. 2011.

〔2〕 http://www.nemc.or.kr/, National Emergency Medical Center.

〔3〕 J. H. Kim, J. S. Cho, Y. S. Lim, S. B. Lee, S. Y. Hyun, J. J. Kim, G. Lee, H. J. Yang, I. Rheu, "The Current State of Airway Management and Ventilation at the Pre-Hospital Stage by Emergency Medical Technicians", Journal of the Korean Society of Emergency Medicine, Vol. 22, No. 2, pp129-141, Apr. 2011.

〔4〕 K. Jung, J. Jang, J. Kim, S. Baek, S. Song, C. Gang, K. Lee, "Delayed Transfer of Major Trauma Patients Under the Current Emergency Medical System in Korea", Journal of the Korean Society of Traumatology, Vol. 24, No. 1. pp25-30, Jun. 2011.

〔5〕 D. Lee, S. C. Noh, "A Study of Methodology Based on Role-Based Security Agent Medical Information System Security Architecture Design", Journal of Information and Security Vol. 11, No. 4, Sept. 2011.

〔6〕 J. P. Kim, A. S. Oh, "Design and Implementation of Emergency Medical System based on the Standard of HL7 Message for Utilization of Patient Medical Information", Journal of Korea Multimedia Society Vol. 14, No. 2, pp.295-306, Feb. 2011.

〔7〕 H. H. Kim, J. R. Cho "A design of efficient emergency medical information system using heuristic knowledge", Journal of the Korea Industrial Information System Society, Vol. 18, No. 3, pp.47-56, Jun. 2013.

〔8〕 H. Lee, T. Kim, S. Choi, I. Kim, J. H. Kim, J. W. Kim, "Developing HL7-based Medical Information Architecture", Information System Review Vol. 3, No. 1, Nov. 2001.

〔9〕 S. J. Oh, "Permission-Based Separation of Duty Model on Role-Based Access Control", The Journal of Information Processing Society Vol. 11-C, No.6, Dec. 2004.

〔10〕 J. Park, "Medical Telecommunication", FORNURSE, Feb. 2010.

〔11〕 Y. Kang, Y. Choi, "Current Status of Information Security against Cyber Attacks in Universities and Its Improvement Methods", Journal of The Korea Society of Computer and Information, Vol. 16, No. 12, Dec. 2011.

〔12〕 Y. Jeun, "The Medical Information Protection and major Issues", Journal of The Korea Society of Computer and Information, Vol. 17, No. 12, Dec. 2012.

〔13〕 Anantharaman, V., Han, L.S, "Hospital and emergency ambulance link: using IT to enhance emergency pre-hospital care", International Journal of Medical Informatics, Vol. 61, pp.147-161, May. 2001.

〔14〕 Andrade, R., von Wangenheim, A., Bortoluzzi, M.K., Comunello, E., "Using mobile wireless devices for interactive visulization and analysis of DICOM data", IEEE Symposium on Computer-Based Medical Systems, Jun. 2003.

〔15〕 B. Orguna, J. Vub, "HL7 Ontology and Mobile Agents for Interoperability in Heterogeneous Medical Information Systems", Computers in Biology and Medicine, Vol. 36, No. 7, pp817-836, Jul. 2006.

〔16〕 R. Sandhu, "The ARBAC97 model for role-based administration of roles", ACM Transactions on Information and System Security, Vol. 2, pp105-135, Feb. 1999.

저 자 소 개

김 형 훈

1986: 전남대학교
계산통계학과 이학사.
1988: 한국과학기술원
전산학과 공학석사.
2007: 한양대학교
전자통신컴퓨터공학과 공학박사
현 재: 광주여자대학교
보건의료시스템공학과 교수
관심분야: 의료정보시스템, 인공지능,
정보보안, 웹프로그래밍
Email : hhkim@kwu.ac.kr

조 정 란

1987: 전남대학교
계산통계학과 이학사.
1989: 전남대학교
전산학과 이학석사.
1999: 전남대학교
전산학과 이학박사
현 재: 광주여자대학교
보건의료시스템학과 교수
관심분야: 보건의료데이타베이스,
정보처리 및 통계분석,
멀티미디어컨텐츠서비스
Email : jrcho@kwu.ac.kr