J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr
Copyright ⓒ 2018 KSII

스마트폰을 활용한 SMS 공증 시스템☆

An SMS Notarization System Using Smartphones

이 윤 호1*
Yunho Lee

요 약

전자공증이 시행된지 10년 가까이 지났지만, 촉탁인 또는 그 대리인이 공증 사무소에 직접 방문해야 하는 번거로움 등으로 인해 활용도는 높지 않은 실정이다. 이에 법무부는 최근 법 개정을 통해 화상공증을 도입함으로써 전자공증의 활성화를 도모하고 있다. 이와 함께 스마트폰의 보급 확대로 개인의 간단한 의사표시나 약속에 휴대폰 SMS 메시지를 이용하는 경우가 많지만, 법적 분쟁 발생 시 해당 메시지의 증거 능력에 대한 법원의 판단은 사안에 따라 다르게 내려지고 있다. SMS 메시지의 증거 능력을 확보하기 위해 SMS 메시지를 전자공증하는 방법을 생각할 수 있으나 이 경우 SMS 메시지를 전자문서화해야 하는 번거로움이 있다.

이러한 문제를 해결하기 위해 본 논문에서는 스마트폰을 이용한 SMS 공증시스템을 제안하고자 한다. 제안한 시스템은 신뢰할 수 있는 공증서버를 이용하며, 공증 요청자에 따라 발신공증 시스템과 수신공증 시스템으로 구분된다.

☞ 주제어 : SMS, 공증, 단문메시지, 모바일메시지, 스마트폰

ABSTRACT

Although it's been nearly decade since the electronic notarization system enforced, the utilization is not high because of the troublesomeness of the client or his agent to visit the notarial office directly. Recently, the ministry of justice introduced e-notary based on audio-visual conference through amendament of the notarial law, and hence it will vitalize the usage of e-notary. In addition, due to the spread of smartphones, many people use SMS messages to express simple statements or promises. However, in case of legal disputes, the judgment of the court is different according to the case. The electronic notarization system can be used to prove of evidence of SMS messages, however, there is a hassle to convert SMS messages to electronic documents.

To solve this problem, this paper proposes an SMS notarization system using smartphones. The proposed system uses reliable notarization server and it is divided into notarization system for message senders and notarization system for message receivers according to notary requestor.

☞ keyword : SMS, Notarization, Short messages, Mobile messages, Smartphones

1. 서 론

공증이란 특정 사실 또는 법률관계의 존부를 공적 권위로써 증명하는 행정행위이며, 일반적으로 국가로부터 임명을 받은 개인 또는 지정된 단체나 그 밖의 기관이 법이 정한 일정한 사항을 증명하여 주는 것을 의미한다[1,2].

공증은 다양한 분야에서 폭넓게 활용되고 있는데, 일상적으로 자주 접하는 각종 계약서나 합의서, 각서, 진술서 등에 주로 활용되며, 최근에는 유언공증도 증가하는 추세에 있다[3].

특히 어음이나 금전소비대차계약을 공정증서로 남겼을 때, 채무자가 돈을 갚지 않을 경우 재판절차 없이 강제집행이 가능하게 되는 등 불필요한 소송 비용을 절감할 수 있다.

이렇듯 공증은 '진정성 보장', '강력한 증거보전', '증거의 무료보관', '신속 · 간편한 권리행사' 및 '비용절감' 등의 장점이 있는데[2], 이를 정리하면 다음 표 1과 같다.

하지만, 선진국과 달리 우리나라는 공증이 활발하지 않은데, 이는 호의에 기초한 거래가 많아 증거를 남기지 않는 문화적 특성에 기인한 것으로 추정되며, 이로 인해 일본과 비교했을 때 형사고소는 170배, 민사고소는 5배가 많을 정도로 각종 민 · 형사 소송이 빈번하게 발생하고 있다[4].

1 Department of Cyber Security & Police, Gwangju University, 277 Hyodeok-Ro, Nam-Gu, Gwangju, 61743, Korea.
* Corresponding author (leeyh@gwangju.ac.kr)
[Received 17 July 2018, Reviewed 20 July 2018(R2 6 August 2018), Accepted 16 August 2018]
☆ 이 연구는 2018년도 광주대학교 대학 연구비의 지원을 받아 수행되었음

(표 1) 공증의 장점
(Table 1) The advantages of notarization

장점	내용
진정성 보장	공정증서의 작성 시 진정을 손상하는 일체의 행위는 범죄행위로 규제하여 엄벌하고 있고, 공정증서의 작성방법 또한 공증인법으로 엄격히 규정되어 있음
강력한 증거보전	공정증서에 기재된 내용은 법적으로 강력히 증명되므로, 사후에 당사자 간 분쟁의 여지가 없으며, 공적인 모든 절차에서 강력한 효력이 있음
증거의 무료보관	공증서류는 공증인서류보존규칙에 의하여 공증인 사무소에 장기간(20년) 무료로 보관
신속・간편한 권리행사	일정한 금액의 지급에 관하여 약정기일 후에는 재판 절차를 거치지 않고 즉시 강제집행을 할 수 있음
비용 절감	재판절차는 기술, 시간, 비용 등이 많이 필요하게 되지만, 공증절차는 신속하고 간편할 뿐 아니라, 비용이 매우 적게 듦

법무부는 개인 및 기업 간 상거래에서 전자적인 방식으로 문서가 교환되는 등 많은 양의 전자문서가 작성되고 통용되는 현실을 반영하기 위해 2009년 2월 6일 「공증인법」 개정을 통해 2010년 8월 7일부터 전자공증제도를 시행하고 있다.

전자공증이란 일정한 시설 등의 요건을 갖춰 법무부장관으로부터 별도 지정을 받은 공증인('지정공증인')이 MS 워드, PDF 등 전자문서 및 종이문서를 스캔한 전자화문서에 전자적 방식으로 공증을 하는 것을 의미[5]하며, 절차는 다음 표 2와 같다.

(표 2) 전자공증의 절차
(Table 2) The procedures for e-notarization

단계	내용
공인인증서 발급	전자서명을 위한 공인인증서 발급
회원가입/로그인	http://enotary.moj.go.kr/ 사이트 회원 가입 및 로그인
촉탁신청	촉탁인이 사서증서/정관/의사록 등의 인증 신청
동일정보 제공신청	사서증서/정관/의사록 등의 동일 정보제공 신청
동일성 검증	공증받은 전자문서를 검증
PDF 변환 및 전자서명	공증받을 파일을 변환/병합하여 첨부 후 전자서명

현재 전자공증 대상 문서는 사서증서, 의사록, 정관 등에 한정되어 있으며, 확정일자를 추가할 예정으로 있다. 하지만, 전자공증은 공증의 대상을 전자문서 및 전자화문서로 확대하였다는 긍정적인 측면에도 불구하고 이용률은 극히 저조한 실정이다. 여러 이유가 있겠지만, 가장 큰 이유는 공증사무소에 촉탁인이나 그 대리인이 반드시 출석하여야 한다는 점인데, 이런 이유로 오히려 전자공증 시스템이 기존 공증시스템보다 불편하다고 여길 수도 있다[6,7].

2013년 전병서는 전자공증에서 공증행위 자체가 전적으로 사이버공간에서 이루어지는 것은 아닌바, 공증의 대면(면전성) 요건에 있어서 일반공증과 전자공증 사이에 아무런 차이가 없는 등 편리성에서 전자공증에 대한 유인책이 전혀 없다는 점을 거론하면서 대면성이라는 기본원칙이 완전히 무시되어서는 안되지만 화상 웹기반 대화 또는 지문인식 등 물리적 실재 조건의 충족 등 대면 요건의 완화 방안을 제시한 바 있다[7].

이 후 2015년 이상진은 화상공증 도입 방안에 대한 법무부 연구보고서[8]를 발표하였으며, 2016년 전병서는 동일한 주제에 대해 법적 해결방안을 제시하였다[9].

최근 법무부는 2017년 12월 12일, 「공증인법」의 제66조의5제2항, 제66조의6제2항 및 제66조의12를 신설하여 인터넷 화상장치를 이용한 인증제도를 도입[10]하는 등 대면요건을 완화함으로써 전자공증이 보다 활성화될 것으로 기대되고 있다.

2. SMS 공증

2.1 SMS 공증의 필요성

현대 사회에서는 스마트폰 등 모바일 기기의 폭발적인 보급 확대로 간단한 의사표시나 개인간 약속은 휴대폰 SMS나 모바일 메신저를 이용하는 경우가 많지만, 분쟁 발생시 SMS 메시지의 법적 효력에 대한 법원 판단이 사안별로 엇갈리고 있다는 점 때문에 SMS 공증의 필요성이 높아지고 있다.

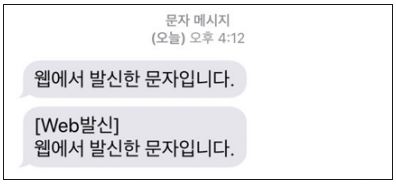
지난 2014년 스웨덴에서 발생한 SMS 유언이 대표적인 사례로, 스웨덴의 한 청년이 자살 전 친구들에게 자신의 재산을 나눠주겠다며 보낸 문자메시지 유언의 효력에 대해 스웨덴 법원은 엇갈리는 판결 끝에 무효로 최종 판단한 바 있다[11].

국내에서도 문자메시지를 읽을 수 있도록 휴대전화기 화면에 표시하여 촬영한 사진의 증거능력에 대한 다툼이 있었는데, 2006년 1심에서는 증거능력을 인정하지 않았지만[12], 2008년 대법원에서는 증거로 사용할 수 없다고

한 원심판결을 파기[13]하는 등 같은 사안을 두고 판결이 엇갈리고 있다.

SMS 발신 및 수신 사실과 메시지 내용에 대한 증명은 SMS 전송을 담당하는 이동통신사가 맡는 것이 가장 확실하지만, 우리나라의 이동통신사는 2005년 이후 메시지 내용을 저장하지 않고 있으며, 발신 및 수신 이력도 최대 1년까지만 보관하기 때문에 증거를 확보하기에는 한계가 있다.

또한, 웹발신 기능을 이용하면 SMS 메시지의 발신자를 임의로 지정할 수 있기 때문에 메시지를 수신한 것만으로 발신자를 특정하기에는 무리가 있다. 물론 웹발신의 경우 이동통신사에서 별도의 서비스를 통해 "[Web발신]"을 추가하여 발신자가 다를 수 있음을 알리고 있지만 사용자가 해당 서비스를 해지하였거나, 일부 웹발신의 경우 "[Web발신]"이 추가되지 않는 경우도 있다. 그림 1은 웹에서 발신한 메시지를 수신한 화면으로 하나에만 "[Web발신]"이 추가된 것을 볼 수 있다.



(그림 1) 웹발신 SMS 메시지
(Figure 1) SMS messages sent by web

따라서 "[Web발신]" 표시가 없다고 해도 발신자를 특정할 수 없는 한계가 있다. 반면, 메시지를 보내는 경우 지정된 수신자에게 메시지를 보냈다는 사실은 증명할 수 있지만, 수신자의 수신 사실은 증명할 수 없는 한계가 있다. 이와 함께 메시지를 발신 또는 수신한 스마트폰을 분실하거나 교체한 경우 관련 사실을 증명하는 것은 더욱 어려워진다.

SMS 메시지에 대해 전자공증을 이용하는 것도 고려할 수 있지만, SMS 메시지를 전자 문서로 다시 작성하는 과정이 필요하기 때문에 간단한 SMS 메시지의 경우 전자공증과는 별도의 공증 방식을 적용하는 것이 보다 효율적일 것이다.

2.2 SMS 공증 시스템

본 논문에서는 간단한 구두계약을 대체하기 위해 SMS 메시지를 활용하는 빈도가 높아지는 현실을 반영한 SMS 공증 시스템을 제안하고자 한다.

본 논문에서 사용할 표기법은 다음 표 3과 같다.

(표 3) 표기법
(Table 3) Notations

표기	설명
A	SMS 발신자
B	SMS 수신자
N	신뢰할 수 있는 공증서버
C	SMS 수/발신자 스마트폰에 설치된 공증 클라이언트로서, 공증서버 N과 통신하여공증 과정을 진행
P_A	SMS 발신자의 전화번호
P_B	SMS 수신자의 전화번호
T	SMS 수/발신 시간
M	공증 대상 메시지
$h(\bullet)$	암호학적으로 안전한 해시함수
$f(\bullet)$	임의의 비트열을 입력받아 지정된 길이의 10진수 숫자를 출력하는 함수
r	공증서버에서 생성한 인증코드(난수)
K	$f(h(P_A, P_B, T, M, r))$ 연산을 거쳐 생성된 인증키

SMS 공증 시스템은 SMS 발신자 A, SMS 수신자 B 및 공증서버 N으로 구성되며, SMS 발신자가 공증을 요청하는 발신공증 시스템과 SMS 수신자가 공증을 요청하는 수신공증 시스템으로 구분할 수 있다. 이와 함께 발신자 및 수신자는 자신의 스마트폰에 공증 클라이언트 C를 설치해야 하는데, 발신공증 시스템의 경우 발신자의 스마트폰에는 반드시 공증 클라이언트가 설치되어 있어야 하며, 수신공증 시스템의 경우 수신자의 스마트폰에는 반드시 공증 클라이언트가 설치되어 있어야 한다.

2.2.1 회원 가입 및 로그인

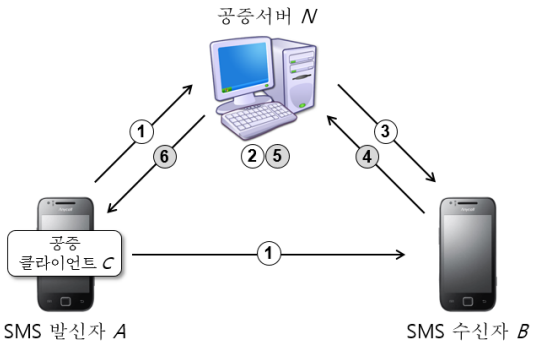
SMS 공증 시스템의 이용자는 모두 사전에 회원 가입을 하여야 하며, 공증 요청자는 로그인 과정을 거쳐 신원 확인을 마쳐야 한다. K뱅크나 카카오뱅크와 마찬가지로 회원 가입은 신분증이나 은행 계좌 확인 등의 신원 확인 후 SMS 인증을 통해 전화번호를 등록함으로써 완료하며, 지문, 패턴, 비밀번호 등의 수단을 이용하여 로그인할 수 있다. 이 후 설명하는 발신 및 수신공증 시스템은 모두 공

증 요청자가 로그인 절차를 완료했다고 가정한다.

이러한 회원 가입 및 로그인 절차는 「공증인법」에서 정한 대면요건을 충족하지는 못하지만, 향후 법개정 가능성도 있으며, 법적 요건을 다루는 것은 본 논문의 범위를 벗어나는 주제이다.

2.2.2 SMS 발신공증 시스템

SMS 발신공증 시스템은 내용증명 우편과 유사한 시스템으로 단문 메시지의 발신 사실을 공증서버가 증명하게 되며, 절차는 다음 그림 2와 같다.



(그림 2) SMS 발신공증 시스템

(Figure 2) A notarization system for message senders

1단계) A가 공증 메시지 M을 작성하고 C를 이용하여 공증요청하면, C는 B에게 해당 메시지를 전송하고 N으로 P_A, P_B, M, T를 전송

2단계) N은 임의의 난수로 구성된 인증코드 r 을 생성한 후 $H = h(P_A, P_B, T, M, r)$와 인증키 $K = f(H)$를 계산

3단계) N은 B에게 인증키 K를 전송함과 동시에, A가 M에 대해 발신공증을 요청하였음을 알리고, 동의할 경우 K를 공증서버에 재전송할 것을 요청

4단계) B는 M에 동의할 경우 N에게 K를 재전송

5단계) N은 B가 전송한 인증키 및 P_B를 검증한 후, 공증 데이터베이스에 P_A, P_B, T, M, r, K를 등록

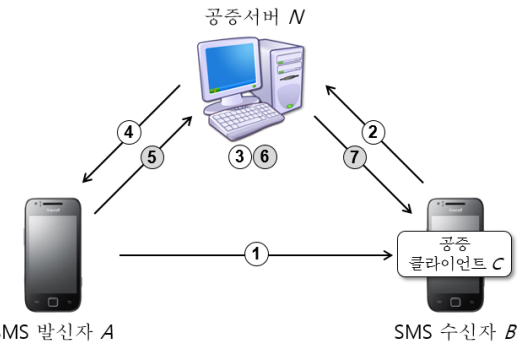
6단계) N은 A에게 공증처리가 완료되었음을 통보

위 4단계)에서 B가 M에 동의하지 않거나 M을 수신하지 못하였을 때 K가 재전송되지 않을 수 있는데, 이 경우 N은 일정시간 대기한 후 A가 B에게 M을 전송한 사실만을 증명할 수 있으며, 이는 내용증명 우편과 같은 기능이라고 할 수 있다.

발신공증 시스템에서 B의 스마트폰에는 공증 클라이언트가 설치되어 있지 않아도 무관하지만, A의 스마트폰에는 반드시 공증 클라이언트 C가 설치되어 있어야 한다.

2.2.3 SMS 수신공증 시스템

SMS 수신공증 시스템은 메시지 M을 수신한 B가 공증요청하는 경우이며, 절차는 다음 그림 3과 같다.



(그림 3) SMS 수신공증 시스템

(Figure 3) A notarization system for message receivers

1단계) A가 B에게 메시지 M을 전송

2단계) B는 C를 이용하여 N에게 P_A, P_B, M, T를 전송함으로써 수신공증 요청

3단계) N은 임의의 난수로 구성된 인증코드 r 을 생성한 후 $H = h(P_A, P_B, T, M, r)$와 인증키 $K = f(H)$를 계산

4단계) N은 A에게 인증키 K를 전송함과 동시에, B가 M에 대해 수신공증을 요청하였음을 알리고, 동의할 경우 K를 공증서버에 재전송할 것을 요청

5단계) A는 M에 동의할 경우 N에게 K를 재전송

6단계) N은 A가 전송한 인증키 및 P_A를 검증한 후, 공증 데이터베이스에 P_A, P_B, T, M, r, K를 등록

7단계) N은 B에게 공증처리가 완료되었음을 통보

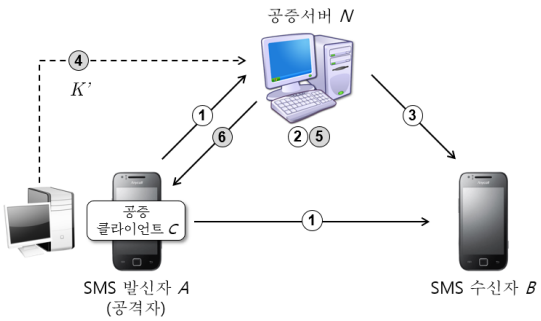
수신공증 시스템에서 A의 스마트폰에는 공증 클라이언트가 설치되어 있지 않아도 무관하지만, B의 스마트폰에는 반드시 공증 클라이언트 C가 설치되어 있어야 한다.

발신공증과 달리 수신공증에서는 5단계)에서 A가 인증키 K를 재전송하지 않을 경우 공증 데이터베이스에 등록하지 않는데, 이는 웹발신 등을 통한 메시지 발신자 위조가 가능하기 때문이다.

3. 안전성 분석

3.1 SMS 발신공증 시스템의 안전성

발신공증 시스템에 대한 공격은 발신자 A가 수신자 B인 것처럼 위장하여 거짓 동의하는 것을 의미하며, 그 과정은 다음 그림 4와 같다.



(그림 4) SMS 발신공증 공격과정

(Figure 4) An attack for notarization of sending short messages

1단계) A가 공증 메시지 M을 작성하고 C를 이용하여 공증요청하면, C는 B에게 해당 메시지를 전송하고 N에게 P_A, P_B, M, T를 전송

2단계) N은 임의의 난수로 구성된 인증코드 r 을 생성한 후 $H = h(P_A, P_B, T, M, r)$와 인증키 $K = f(H)$를 계산

3단계) N은 B에게 인증키 K를 전송함과 동시에, A가 M에 대해 발신공증을 요청하였음을 알리고, 동의할 경우 K를 공증서버에 재전송할 것을 요청

4단계) A는 웹발신 등을 이용하여 발신자를 B로 지정한 후 인증키 K를 N에게 전송

5단계) N은 수신한 인증키를 검증한 후, 공증 데이터베이스에 P_A, P_B, T, M, r, K를 등록

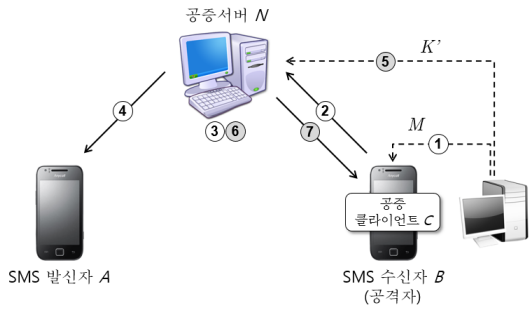
6단계) N은 A에게 공증처리가 완료되었음을 통보

이 공격이 성공하기 위해서는 4단계)에서 A가 K를 생성할 수 있어야 하지만, A는 인증코드 r을 모르기 때문에 K를 생성할 수 없다. 이 경우 r 또는 K를 추측할 수 밖에 없는데, 일반적으로 $|r| > |K|$이므로 성공 확률 p는 K를 정확하게 추측할 확률이 되며, $|K| = 6$이라면, $p = 1/1,000,000$이 된다.

이외에도 발신자 A가 아닌 다른 제삼자가 A인 것처럼 공증을 요청하는 위장공격도 고려할 수 있으나, 지문, 패턴, 비밀번호 등을 이용한 로그인 절차가 안전하다면 이러한 공격은 사실상 불가능하다.

3.2 SMS 수신공증 시스템의 안전성

수신공증 시스템에 대한 공격은 수신자 B가 발신자 A인 것처럼 위장하여 자신에게 M을 전송하고 거짓 동의하는 것을 의미하며, 그 과정은 다음 그림 5와 같다.



(그림 5) SMS 수신공증 공격과정

(Figure 5) An attack for notarization of receiving short messages

1단계) B는 웹발신 등을 이용하여 발신자를 A로 지정한 후 M을 자신에게 전송

2단계) B는 C를 이용하여 N에게 P_A, P_B, M, T를 전송함으로써 수신공증 요청

3단계) N은 임의의 난수로 구성된 인증코드 r 을 생성한 후 $H = h(P_A, P_B, T, M, r)$와 인증키 $K = f(H)$를 계산

4단계) N은 A에게 인증키 K를 전송함과 동시에, B가 M에 대해 수신공증을 요청하였음을 알리고, 동의할 경우 K를 공증서버에 재전송할 것을 요청

5단계) B는 웹발신 등을 이용하여 발신자를 A로 지정한 후 인증키 K를 N에게 전송

6단계) N은 수신한 인증키 및 P_A를 검증한 후, 공증 데이터베이스에 P_A, P_B, T, M, r, K를 등록

7단계) N은 B에게 공증처리가 완료되었음을 통보

이 공격이 성공하기 위해서는 5단계)에서 B가 K를 생성할 수 있어야 하지만, B는 인증코드 r을 모르기 때문에 K를 생성할 수 없다. 이 경우 r 또는 K를 추측할 수 밖에 없는데, 일반적으로 $|r| > |K|$이므로 성공 확률 p는 K를 정확하게 추측할 확률이 되며, $|K| = 6$이라면, $p = 1/1,000,000$이 된다.

4. 결 론

전자공증 제도가 시행된지 10년 가까이 지났지만, 대면 요건 등으로 인해 활용도가 높지 않은 상황에서, 법무부는 화상공증을 도입하는 등 전자공증의 편의성이 높임으로써 활성화를 도모하고 있다. 이와 함께 최근 간단한 의사표시나 개인간 약속은 공식 문서를 이용하지 않고 SMS 메시지를 이용하는 경우가 많지만, 분쟁 발생시 SMS 메시지의 진위 여부나 법적 효력에 대한 법원의 판단은 사안에 따라 다르게 내려지고 있다. 이를 해결하기 위해 SMS 메시지를 전자공증하는 방법을 생각할 수 있지만, SMS 메시지를 전자문서화해야 하기 때문에 번거로운 측면이 있다.

본 논문에서는 이러한 SMS 메시지에 대한 분쟁 해결을 위해 신뢰할 수 있는 제3자를 이용하는 SMS 발신공증 및 수신공증 시스템을 제안하였다. 제안한 시스템은 SMS 메시지의 발신자 및 수신자가 모두 동의한 경우 공증서버에 관련 정보를 서버에 보관하여 추후 사실 관계 증명에 활용할 수 있어 법적 분쟁 해결에 기여할 것으로 기대된다.

참고문헌(Reference)

[1] Wikipedia, “Notarization,” https://ko.wikipedia.org/wiki/공증, accessed Mar. 29, 2018.

[2] Law Firm Hanmi, “What is Notarization,” http://lawhanmi.com/what-is-notary/, accessed Mar. 29, 2018.

[3] Lawtimes, “The reason why elders prefer ‘testament notarization’,” https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=78387, 2013.

[4] Lawtimes, “Notarization is a solution to our social conflict prevention,” https://www.lawtimes.co.kr/ Legal-News/Legal-News-View?serial=78482&page=6, 2013.

[5] Ministry of Justice, “Electronic notary system,” http://enotary.moj.go.kr/, accessed Mar. 29, 2018.

[6] Ministry of Justice, “Activation of electronic notarization,” Research Report, 2013.

[7] Byungseo Chon, “Some issues in electronic notarization,” Civil Procedure, Vol. 17, No. 2, pp. 555-576, 2013. http://www.dbpia.co.kr/Article/NODE02319281

[8] Ministry of Justice, “A Study on e-notary based on audio-visual conference,” Research Report, 2015.

[9] Ministry of Justice, “Legal solutions for e-notary based on audio-visual conference,” Research Report, 2016.

[10] Ministry of Government Legislation, “공증인법,” http://www.law.go.kr/법령/공증인법, accessed Aug. 06, 2018.

[11] Lawtimes, “Does ‘SMS testament’ work... What is the judgment of the court?,” https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=82765, 2014.

[12] The Hankyoreh, “Photographed text messages cannot be used as evidence,” http://www.hani.co.kr/arti/society/society_general/114156.html, accessed Aug. 06, 2018.

[13] Law Firm Oasis, “Evidence of photographed text messages stored on mobile phones,” http://lawoasis.co.kr/법률칼럼/1272402, accessed Aug. 06, 2018.

◐ 저 자 소 개 ◑

이 윤 호(Yunho Lee)
1991년 성균관대학교 정보공학과 졸업(학사)
1993년 성균관대학교 정보공학과 졸업(석사)
2008년 성균관대학교 컴퓨터공학과 졸업(박사)
1993년~2000년 한국통신(KT) 연구개발본부 전임연구원
2000년~2005년 KBS인터넷(주) 기술지원팀장
2004년~2005년 ㈜뱅크타운 책임연구원
2008년~2011년 성균관대학교 컴퓨터공학과 연구교수
2011년~현재 광주대학교 사이버보안경찰학과 교수
관심분야 : 전자투표, 컨텐츠보안, 시스템보안, 응용보안 등
E-mail : leeyh@gwangju.ac.kr