

<http://dx.doi.org/10.17703/JCCT.2022.8.3.559>

JCCT 2022-5-70

안전한 모바일 전자고지서비스를 위한 민간기관과 본인확인기관 간의 연계정보 일괄변환 기술기준 개발에 관한 연구

A Study on the Development of Technology Standards for the Batch Conversion of CI between Private and Personal Identity Proofing Organizations for Safe Mobile Electronic Notification Service

김종배*

JongBae Kim*

요약 모바일 기기의 확산으로 이용자가 소지하고 있는 모바일 기기와 이용자 식별을 통해 전자고지문을 이용자의 모바일 기기로 전송하여 전자고지문의 송달증명과 유통증명을 수행하는 모바일 전자고지서비스 이용 증가하고 있다. 이때 모바일 기기 단말기 소유자와 고지문 수신자를 식별하기 위해 연계정보를 사용한다. 따라서 본 연구에서는 모바일 전자고지문 발송요청기관이 본인확인기관에게 전자고지문 수신자의 주민등록번호를 연계정보로 일괄변환 요청 시 처리흐름, 연동규격, 관리방안 등을 제안한다. 제안한 방안에서는 민간기관과 본인확인기관 간의 연계정보 일괄변환 처리 절차, 정보 송·수신 방안, 연동규격 등을 정의함으로써 안전한 모바일 전자고지서비스가 가능함을 제시한다. 고지문을 전자적으로 발송함에 있어 수신자 식별의 안전성, 전자고지문의 유출 방지, 전송구간 사이의 데이터 보호 등을 효과적으로 적용할 수 있어 모바일 전자고지서비스의 활성화를 기대할 수 있을 것이다.

주요어 : 모바일 전자고지서비스, 연계정보 일괄변환서비스, 연계정보 연동규격

Abstract Due to the spread of mobile devices, the use of mobile electronic notification services is increasing. For the mobile electronic notification service, the connecting information is required to identify the owner of the mobile device and the recipient of the notification. The connecting information is an online resident registration number, and safe management is essential. Therefore, in this paper, the processing flow, interconnecting standard, and management plan are proposed when a mobile electronic notification requesting agency requests the identity verification agency to convert the resident registration number of the recipient of the electronic notification to connecting information. In the proposed method, it is suggested that a safe mobile electronic notification service is possible by defining the process of collective conversion of connecting information between private organizations and personal identity proofing agency, information transmission and reception methods, and interworking standards.

Key words : Mobile Electronic Notification Service, Connecting Information Batch Conversion Service, Connecting Information Linkage Standard

*정회원, 세종사이버대학교 소프트웨어공학과 교수 (제1저자)
접수일: 2022년 4월 21일, 수정완료일: 2022년 5월 2일
게재확정일: 2022년 5월 6일

Received: April 21, 2022 / Revised: May 2, 2022

Accepted: May 6, 2022

*Corresponding Author: jb.kim@sjcu.ac.kr

Dept. of Software Engineering, Sejong Cyber Univ, Korea

1. 서론

모바일 전자고지서비스는 공인전자문서중계사업자로 하여금 수신자가 소지하고 있는 모바일 기기로 전자 고지문을 발송하는 서비스이다. 이때 종이 기반의 고지문 발송서비스에서 집배원이 수행하는 역할과 같이 송달 및 유통증명을 수행할 수 있도록 공인전자문서중계자가 그 역할을 수행한다 [1-3]. 전통적으로 종이 고지문 송달서비스는 우체국을 통해 대면확인을 거쳐 직접적으로 송달하게 됨으로써 송달증명이라는 법적인 요건을 확보하게 된다. 이때 고지문 수신자와의 대면확인을 위해서는 신분증표와 수령인 서명 등의 방법으로 확인함으로써 이루어진다. 하지만, 종이 기반의 고지문 전송에 있어서 고지문 분실, 개인정보 노출, 대면확인 어려움 등으로 인해 여러 문제점이 발생하고 있다. 특히 최근 1인 가구 수의 증가로 인해 사생활 노출을 꺼리고 있으며 우편물 수신을 거부하거나 수령하지 않는 경우도 빈번히 발생하고 있다 [4]. 이로 인해 종이 우편물들의 상당수가 반송되고 있으며 발송된 우편물들이 우편수신함에 적재된 유출되거나 타인에 의해 열람되어 개인정보 침해 이슈도 발생하고 있다. 그렇다고 종이 고지문 발송을 중단할 수도 없는 것이 사회적인 약자나 IT 소외계층 등을 인해 모든 고지문을 전자적으로만 발송할 수도 없는 상황이다 [5]. 최근 들어서는 종이 사용 억제로 탄소배출 감소 정책으로 인해 친환경 및 저탄소 정부 정책에 부합하기 위해 종이 우편물 발송을 최소화하고 있으며, 이로 인해 모바일 기기를 활용한 정보 전달 체계로 변환을 꾀하고 있다 [6]. 2016년 행정·공공 분야에서 발송된 일반우편과 등기우편은 약 4억 2천만 건으로 우편비용만 2천억 원에 달하고 있으며, 이러한 우편발송을 위해 약 5만 그루의 나무를 사용한 것으로 조사되었다. 여기서 약 5만 그루의 나무에서 종이를 생산하여 우편으로 발송할 때 발생하는 미세먼지 약은 약 1.8톤에 이르고 있으며, 이는 경기도 전역에 발생하는 하루 미세먼지 양의 절반에 이르는 수준이라고 보도한 바 있다 [7]. 국세청의 연도별 우편 고지문 발송 현황을 확인한 결과, 그림 1과 같이 매년 발송 건수 대비 반송율이 약 16% 이상 상회하고 있으며 이로 인해 종이 우편물 생산에 따른 비용과 탄소 배출, 환경오염 등이 사회적인 문제로 대두되고 있다 [8]. 그림 1과 같이 종이 우편물 발송으로 반송율 증가에 따른 비용

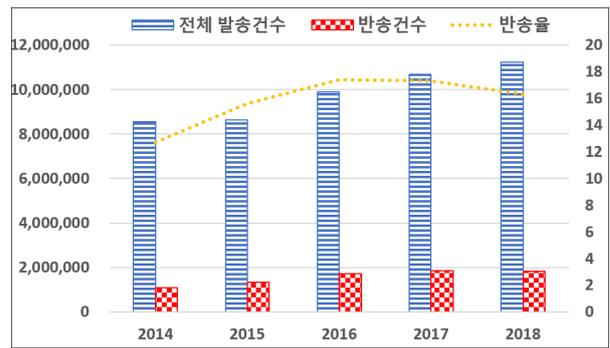


그림 1. 연도별 우편 고지서 발송 현황 (국세청, [8] 재구성)
Figure 1. Status of the number of mails and returns by year

증가 등으로 인해 종이 고지문을 모바일 기기를 활용한 전자고지문으로 전송하는 서비스의 확대가 요구되고 있다 [1]. 전자문서란 정보처리시스템에 의하여 전자적인 형태로 작성·변환되거나 송신·수신 또는 저장된 정보를 의미한다 [9]. 종이 고지문 전송서비스가 가지는 문제점들을 극복하기 위해 최근에는 모바일 기기 기반의 전자고지문 전송서비스가 확대하고 있다. 그림 2는 현재 서비스되고 있는 모바일 전자고지서비스 사례이다. 해당 모바일 전자고지문이 모바일 앱이나 휴대폰 문자 메시지 발송으로 모바일 전자고지문이 저장된 시스템의 접속으로 열람할 수 있다. 이때 수신자는 전자문서 열람 시 본인확인을 거쳐 수신확인을 하게 되고 발송요청기관은 공인전자문서중계자를 통해 전자고지문 발송을 요청함으로써 송달 및 유통증명을 할 수 있게 된다.



그림 2. 모바일 전자고지서비스 사례
Figure 2. Examples of mobile electronic notification services

종이 고지문 발송요청기관이 전자고지문을 발송함에 있어 해당 수신자가 가입하고 있는 온라인 서비스 가입 정보(휴대전화번호, SNS ID 등)가 필요하다. 일반적으로

전자고지문 발송요청기관이 저장하고 있는 수신자 정보는 해당 수신자를 식별할 수 있는 성명, 고유식별정보, 주소 이외에 온라인 서비스 가입 정보를 요구하거나 혹은 수집하고 있지 않는 경우가 대부분이다. 고지문 발송요청기관이 필요에 의해 수신자에게 수집 받은 개인정보 역시 현행화 여부를 확인할 수 없다. 서비스 및 신청 당시 제공받은 개인정보인 연락처, 이메일 정보 등이 실제 고지문 수신자 정보인지 확인할 수 없는 문제점이 있다. 결국, 전자고지문 발송요청기관은 수신자들에게 온라인 가입 정보(SNS 아이디, 휴대전화 번호 등)를 요구하게 되고 수신자는 해당정보의 제공을 거부하거나 변경 시 이를 다시금 갱신해야 하는 한계점이 있다. 더구나 전자고지문 발송기관에서 다량의 고지문을 발송하는데 많은 수신자들에게 온라인 서비스 가입정보를 요구할 수 없는 한계가 있다. 결국 고지문 발송요청기관은 종이 고지문을 발송하여 송달증명을 입증 받은 방법이 최선책으로 이용되고 있는 실정이다. 전자고지문으로 관련 정보를 전달하는 서비스는 과거부터 진행되고 있었다. 신용카드 명세서, 공공요금 고지서, 법칙금 고지서 등은 이용자가 사전에 본인확인을 거친 후 자신의 온라인 서비스 가입정보를 제공함으로써 수신 받을 수 있다. 이러한 서비스는 수신자의 요구에 따라 직접 현행화된 정보를 제공한 것으로서 발송요청기관은 수신자가 제공한 정보를 기반으로 전송하여 송달 처리를 이행할 수 있다. 이러한 전자문서고지서서비스를 위해서는 전자문서를 전달받아 발송처리를 수행하는 공인전자문서중계자가 필요하다. 공인전자문서중계자는 과학기술정보통신부로부터 법적인 지휘를 부여받아 공식적으로 전자문서를 발송요청기관으로부터 전달받아 수신자의 온라인 가입정보를 기반으로 전자고지문 발송·송달증명·신원확인 등을 수행한다. 최근 들어 저탄소 정책, 환경보호, 개인정보 노출 방지 등의 사회적 분위로 인해 종이 고지문을 전자고지문 발송으로 전환하고 있으며, 특히 공공·행정기관이 주도적으로 시행하고 있고, 현재는 민간기관(은행, 보험사 등)들도 전자고지서서비스를 확대하고 있다. 그림 3은 공인전자문서중계자를 통한 전자문서 유통 건수를 나타낸 그림이다.

모바일 기반의 전자고지서서비스를 위해서는 그림 4와 같이 발송요청기관, 발송처리기관, 수신자 그리고 본인확인기관으로 구성되어 있다. 발송요청기관은 전자고지문 발송을 요청하는 기관이고, 발송처리기관은 실제

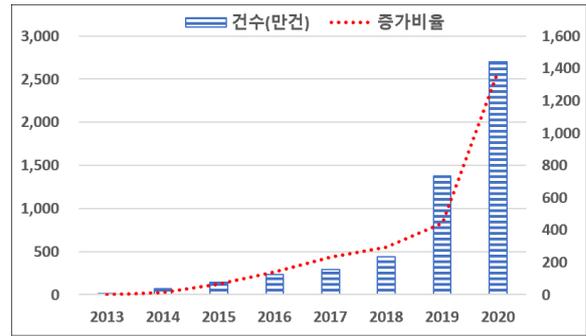


그림 3. 공인전자문서중계자를 통한 전자문서 유통 건 수 (과학기술정보통신부)
 Figure 3. Status of the number of electronic documents distributed by authorized electronic document intermediary

전자고지문을 수신자가 가입한 온라인 서비스 가입정보를 기반으로 발송하고 송달과 유통증명, 그리고 수신자 식별 및 확인 업무를 처리하는 기관이다. 그리고 본인확인기관은 발송요청기관이 보유한 주민등록번호를 연계정보로 변환하는 업무를 처리하는 기관이다.

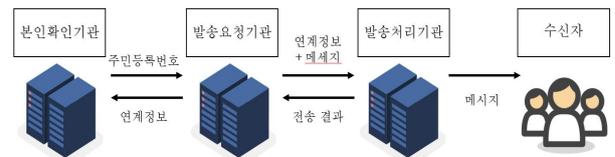


그림 4. 모바일 전자고지서서비스 처리 흐름도
 Figure 4. Flow of mobile electronic notification service processing

그림 4에서 본인확인기관이 필요한 이유는 발송요청기관은 수신자의 고유식별정보인 주민등록번호는 수집·저장하고 있으나 온라인 서비스 가입정보는 보유하고 있지 않다. 그리고 발송처리기관은 공인전자문서중계사업자로서 민간기관이고 법적으로 온라인 서비스 가입자의 주민등록번호를 수집할 수 없다. 유일하게 온라인 서비스 가입자 회원가입, 결제, 배송 등을 위해 본인확인을 요구하고 수집 받은 연계정보(Connecting Information, 이하 'CI')를 저장하고 있다. 따라서 발송요청기관과 발송처리기관 간의 고지문 수신자 식별을 위해서는 CI를 두 기관과 공유하는 것이 필요하다. 따라서 전자고지문 발송요청기관이 저장하고 있는 주민등록번호를 CI로 변환하는 것이 필요하다. 국내에서 CI를 생성할 수 있는 기관은 방송통신위원회로부터 주민등록번호 대체수단으로 본인확인서비스를 제공하는 기관으로 지정받은 본인확인기관이다. 결국, 발송요청기관은 수신자의 주민

등록번호를 본인확인기관에게 제공하고 본인확인기관은 주민등록번호에 대응하는 CI를 생성하여 발송요청기관에게 제공하는 과정이 필요하다. 하지만, 법적인 규제로 인해 수신자의 고유식별정보를 제공하기 위해서는 사전에 수신자의 동의가 필수적이고, CI 제공 역시도 개인정보로써 수신자의 동의가 필수적이다. 이러한 법적인 규제를 임시로 허용하여 수신자의 편익이 개인정보 침해보다 높다는 판단하여 ICT 규제샌드박스에서 수신자의 사전 동의 없이 CI의 변환을 임시적으로 허용하였다. 하지만 수신자의 CI는 온라인상의 주민등록번호와 같은 성격으로써 안전한 관리와 보호가 필요하며, CI를 사용하는 각 기관들이 표준화된 방법으로 관리하는 기술기준이 요구된다.

따라서 본 논문에서는 민간기관이 모바일 전자고지서비스를 이용함에 있어 CI의 안전한 활용과 보호를 위한 CI 일괄변환 기술기준을 제시한다. 제안한 기술기준은 개방적이면서도 안전성 및 신뢰성을 확보할 수 있는 방식으로 CI를 변환하는 체계를 구성하기 위해 필요한 구성요소를 정의하고 각 구성요소들 간 연관관계를 체계화하는 것이다. 제안한 기술기준은 CI를 변환하는 체계에 대한 전체 구조와 이를 위해 필요한 구성요소 및 각 구성요소의 역할, 그리고 연계규격, 보안기준을 제안한다.

II. 연계정보(CI) 일괄변환서비스

1. 서비스 정의

CI일괄변환서비스는 모바일 전자고지문 발송요청기관이 전자고지문 발송 목적으로 수신자의 주민등록번호를 CI로 변환하는 서비스이다. CI일괄변환서비스를 통해 발송요청기관은 방송통신위원회로부터 지정받은 본인확인기관에게 수신자의 주민등록번호를 제공하여 CI로 변환할 수 있고, 수신 받은 CI를 활용하여 전자고지문을 발송한다. 본인확인기관은 CI일괄변환시스템을 보유하고 있으며 또한 본인확인서비스를 위해 이용자가 가입한 수신자의 고유식별정보, 즉 주민등록번호와 본인확인기관만 보유하고 있는 비밀정보를 활용하여 CI를 생성한다. 이러한 CI일괄변환시스템은 민간기관이 제공한 주민등록번호를 제공받아 CI를 생성하는 시스템이다. 민간기관에서는 본인확인기관과 공인전자문서중계자에게로 연동전문을 활용하여 모바일 전자고지문 발송서비스를 제공한다. 그림 5는 CI일괄변환서비스와

모바일 전자고지서비스 개요도이다. 본 논문에서는 발송요청기관과 본인확인기관 간의 수신자의 주민등록번호와 CI의 변환, 제공, 처리 등 연동처리에 대한 방안을 제시한다.

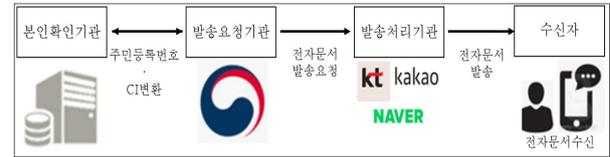


그림 5. CI일괄변환서비스와 모바일 전자고지서비스 개요
Figure 5. Flow of providing mobile electronic notification service through CI batch conversion

2. 서비스 시스템 구성

CI일괄변환서비스 제공을 위해 각 기관이 운영이 필요한 시스템과 각 시스템간의 구성은 그림 6과 같다. 그림 6에서 발송관리시스템은 모바일전자고지서비스를 통해 전자문서를 발송하기 위한 목적으로 발송 대상자의 개인정보(주민등록번호 등)를 관리하는 발송요청기관의 시스템이다. 그리고 CI일괄변환시스템은 모바일 전자고지서비스 목적으로 CI변환을 위해 발송요청기관으로부터 요청받은 주민등록번호를 CI로 변환하고 발송요청기관에게 응답하는 본인확인기관의 시스템이다. 따라서 발송요청기관과 본인확인기관 간의 인터넷 망으로 연결되어 있으며 두 기관 간에는 전송구간 암호화와 전송 데이터의 위변조 방지를 위한 데이터 암호화, HMAC(Hash-based Message Authentication Code) 추가 등이 요구된다.

3. 서비스 프로세스

CI일괄변환서비스를 이용 또는 제공함이 있어 발송요청기관과 본인확인기관 간의 주요한 서비스 프로세스 처리는 다음과 같이 정의할 수 있다.

- ① 발송요청기관은 수신자 주민등록번호를 적재한다.
- ② 발송요청기관은 전자고지문 발송을 위해 수신자의 주민등록번호를 본인확인기관에 전달한다.
- ③ 본인확인기관은 수신자의 주민등록번호를 CI로 변환한다.
- ④ 본인확인기관은 발송요청기관에게 CI를 전달한다.
- ⑤ 발송요청기관은 수신자의 CI를 저장한다.
- ⑥ 발송요청기관은 변환된 CI를 활용하여 모바일 전자고지서비스 위해 발송처리기관에게 전달한다.

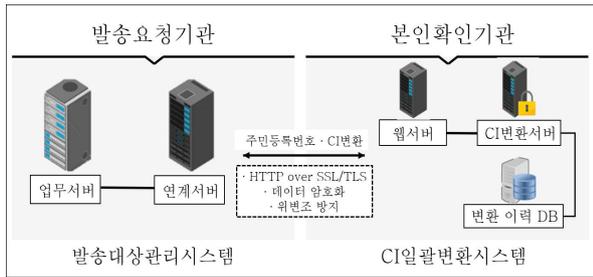


그림 6. CI일괄변환서비스와 처리기관 및 주요 시스템 구성
 Figure 6. Flow of providing user information for sending electronic documents

그림 7은 CI일괄변환서비스를 수행하기 위한 발송요청기관과 본인확인기관 간의 서비스 처리 프로세스이다. 모바일 전자고지문 발송요청기관이 저장하고 있는 수신자의 주민등록번호를 CI로 변환하기 위해 CI일괄변환처리 프로세스와 같이 발송요청기관은 수신자 주민등록번호와 발송요청기관의 식별정보도 함께 전송하는 것이 필요하다. 특히 수신자의 주민등록번호를 공용 인터넷망에 전송 할 시 보호조치를 취하고 전송하는 것도 필요하다. 일반적으로 발송요청기관과 본인확인기관 간에서는 인터넷 전용선으로 구축된 경우보다는 일반 공용 인터넷망을 사용하여 정보를 전송하는 경우가 대부분으로써 두 기관간의 모바일 전자고지를 위한 관련 정보 연동을 위해서는 서로 간의 데이터 암호화와 전송 구간 간의 암호화가 요구된다. 전송 데이터 암호화와 전송 구간 암호화 적용을 위해서는 기관 간 암호화키 교환 절차도 사전에 정의하는 것이 필요하다. 표 1은 그림 7의 CI일괄변환서비스를 수행하기 위해 각 기관별에서 처리하는 세부 프로세스와 각 프로세스에 대한 설명이다. 모바일 전자고지서비스를 제공하기 위해 발송요청기관과 본인확인기관의 수행해야 할 역할을 정의한

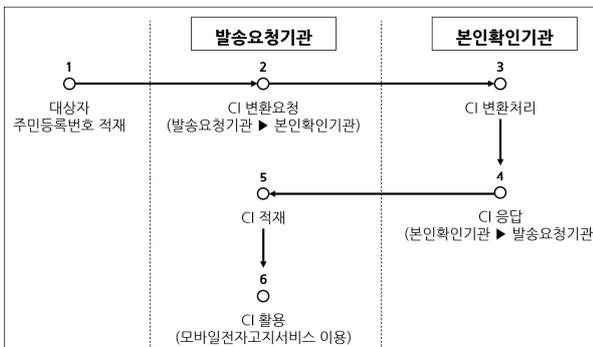


그림 7. CI일괄변환을 위한 단계별 처리 프로세스 흐름
 Figure 7. Flow of processing process by step for CI batch conversion

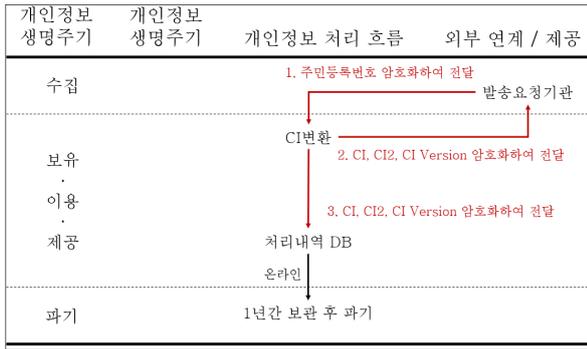
것이다. 표 1의 CI일괄변환 연동처리를 수행의 세부 프로세스를 정의함으로써 안전한 연계정보의 활용이 가능함으로 본 연구에서는 각 세부프로세스들을 정의하고 설계 방안을 제시한다.

표 1. CI일괄변환서비스의 각 단계별 프로세스 및 설명
 Table 1. Process and description of each step of CI batch conversion service

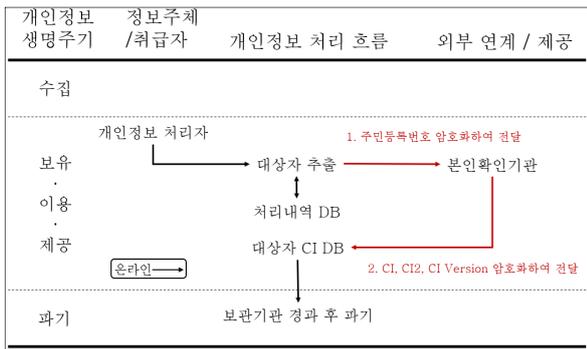
번호	주체	프로세스 명	설명
①	발송요청기관	주민등록번호 적재	발송요청기관은 발송 대상자로부터 모바일전자고지 서비스 이용을 위한 수신자의 주민등록번호를 수집 또는 보관
②	발송요청기관	CI변환요청	발송요청기관은 본인확인기관에 발송 대상자의 주민등록번호를 송신하고 CI변환을 요청
③	본인확인기관	CI변환처리	본인확인기관은 발송요청기관으로부터 전달받은 주민등록번호를 CI로 변환
④	본인확인기관	CI응답	본인확인기관은 변환된 CI 및 처리 결과를 발송요청기관으로 응답한다.
⑤	발송요청기관	CI적재	발송요청기관은 발송 대상자 시스템에 CI정보를 수집 또는 보관
⑥	발송요청기관	CI활용	발송요청기관은 CI일괄변환 서비스를 통해 득한 CI를 활용하여 모바일 전자고지서비스를 통해 수신자에게 전자문서 발송

III. 서비스 개인정보처리 흐름

CI일괄변환서비스 이용 및 제공을 위한 본인확인기관과 발송요청기관에서 처리되는 개인정보처리흐름은 그림 8과 같다. 본인확인기관은 발송요청기관이 모바일 전자고지서비스 이용목적으로 CI변환 요청 시 발송요청기관이 제공한 수신자의 주민등록번호에 대하여 CI로 변환 처리를 수행하고 발송요청기관에게 제공한다. 이후 본인확인기관은 발송요청기관으로부터 전달받은 수신자의 주민등록번호를 즉시 파기하는 것이 필요하다. 관련 법령에 의해 주민등록번호 처리 시 이용자의 동의가 필수적이나 ICT 규제샌드박스의 특별법에 따라 임시적으로 허용되고 있는 바, 수신된 정보는 CI 변환 이후 처리 기록 외에 주요한 개인정보 등은 삭제하는 것이 필요하다. 특히, CI 역시 본인확인기관에서는 CI의 생성·관리하고 주민등록번호의 처리하는 등의 중요성으로 인해 CI의 저장을 금지하고 있다. 본인확인기관은 발송



(가)



(나)

그림 8. 모바일 전자고지서비스 개인정보 처리 흐름도, (가)본인확인기관 개인정보처리흐름도, (나)발송요청기관 개인정보처리 흐름도

Figure 8. Flow of personal information processing on mobile electronic notification service. (a) personal identity proofing agency, (b) the requesting agency

요청기관의 처리내역 목적으로 CI변환처리 이력을 일정기간 저장한다. 이때, 본인확인기관이 모바일 전자고지서비스 목적으로 CI 저장 시 관련 정보의 안전한 보호조치 이후 분리하여 보관하는 것이 필요하다. 그리고 발송요청기관의 개인정보 취급자는 모바일 전자고지서비스를 통해 전자문서를 발송할 수신자의 주민등록번호를 추출하여 본인확인기관에 CI변환을 요청한다. 이때 변환된 CI는 보관기관이 경과 시, 지체 없이 파기하는 것이 필요하다.

IV. CI일괄변환서비스 기술기준

모바일 전자고지서비스를 위해 발송요청기관과 본인확인기관 간의 CI의 변환 요청이 필요하다. 이러한 CI 변환을 위해서는 모바일 전자고지문 수신자의 주민등록번호를 발송요청기관이 본인확인기관으로 제공하고, 본인확인기관은 수신 받은 주민등록번호를 이용하여 CI로

변환한다. 그리고 본인확인기관은 CI를 발송요청기관에 제공하는 과정이 CI일괄변환 처리 과정이다. 이러한 처리를 수행하기 위해 모바일 전자고지서비스 제공을 위한 기술기준을 본 연구에서 제안한다. 본 연구에서 제안한 CI일괄변환 서비스를 위한 각 세부 프로세스별 기술사항은 다음과 같다.

1. 변환요청 프로세스 기준

모바일 전자고지문 발송요청기관이 CI변환을 위해 본인확인기관에 수신자의 주민등록번호를 전달하는 프로세스는 그림 9와 같다.

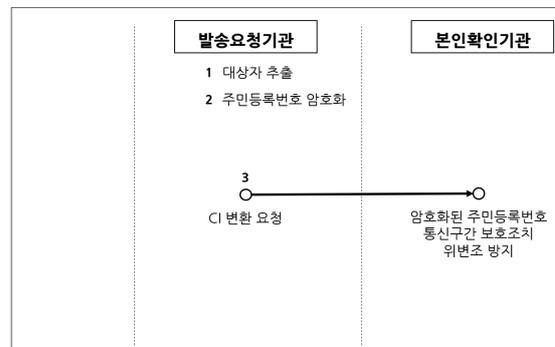


그림 9. CI일괄변환 요청 프로세스

Figure 9. Process for CI batch conversion requests

발송요청기관은 전자고지문 발송 대상자를 선정하고 해당자의 주민등록번호를 추출한다. 그리고 추출한 주민등록번호를 본인확인기관과 협의한 암호화 프로세스에 따라 데이터 암호화와 전송구간 암호화를 적용한 후 본인확인기관에게 전송한다. CI변환 요청을 위한 세부 처리 프로세스 기준 정의는 표 2와 같이 제시한다.

표 2. CI일괄변환 요청의 각 단계별 프로세스 및 설명

Table 2. Process and description of each step of CI batch conversion requests

순번	주체	프로세스 명	설명
①	대상자 추출	발송 요청 기관	전자문서 유통 플랫폼을 통해 전자문서를 발송할 수신자의 주민등록번호를 추출한다.
②	주민등록번호 암호화	발송 요청 기관	추출한 대상자의 주민등록번호를 본인확인기관과 사전에 협의한 방식으로 암호화한다.
③	CI변환 요청	발송 요청 기관	암호화된 주민등록번호를 전송, 본인확인기관에 CI변환을 요청한다. (데이터는 본인확인기관과 사전에 협의한 방식으로 통신구간 보호조치를 적용하여 전송하여야 한다.)

2. 서비스 프로세스 기준

본인확인기관이 발송요청기관으로부터 전달받은 모바일 전자고지문 수신자의 주민등록번호를 CI로 변환하는 프로세스는 그림 10과 같다.



그림 10. CI일괄변환 요청 시 본인확인기관의 처리 프로세스
 Figure 10. Processing by the personal identity proofing agency when requesting CI batch conversion

표 3. CI일괄변환 요청 시 본인확인기관의 처리 프로세스 및 설명
 Table 3. Process and description of each step of CI batch conversion requests by the personal identity proofing agency

순번	프로세스 명	처리 주체	설명
①	발송요청기관검증	본인확인기관	CI변환 요청이 실제 발송요청기관으로부터 발생한 정당인지 발송요청기관코드 확인, 시스템 접근권한 부여 등 전자적인 방법을 통해 검증한다.
②	요청정보수신	본인확인기관	주민등록번호 등 발송요청기관으로부터 요청받은 CI변환처리를 위한 정보를 수신 및 확인한다.
③	요청정보복호화	본인확인기관	발송요청기관으로부터 수신한 주민등록번호를 사전에 협의한 방식으로 복호화 한다.
④	CI변환처리	본인확인기관	발송요청기관으로부터 수신한 주민등록번호를 CI변환모듈을 통해 변환한다. (이때, CI변환을 완료한 주민등록번호는 목적달성 후 즉시 파기하여야 한다.)
⑤	처리내역보관	본인확인기관	CI변환처리 일시, 발송요청기관정보, 변환 처리된 CI 등 CI변환 처리내역을 저장한다.
⑥	CI암호화	본인확인기관	변환이 완료된 CI를 발송요청기관과 사전에 협의한 방식으로 암호화 한다.

본인확인기관에서는 CI일괄변환 요청한 발송요청기관이 정당한 기관인지 검증하고, 전달받은 정보에 대한 검토를 통해 암호화된 주민등록번호를 복호화하고, 주민등록번호를 사용하여 CI정보를 변환 처리하는 과정을 수행한다. 각 처리 내역에 대한 이력을 보관하고 다시금 CI를 암호화하여 이용기관에게 전송한다. 이때 저장하는 정보는 발송요청기관, 요청일시, 제공일시 정보 등을 저장하고 그 외 고유식별정보와 연계정보는 저장하지 않도록 한다. 표 3은 본인확인기관이 CI변환 요청처리 프로세스 세부 기준을 나타낸 것이다.

3. 결과확인 프로세스 기준

본인확인기관이 CI변환 처리가 완료된 CI를 발송요청기관에 응답하고 발송요청기관이 CI변환과 관련된 결과를 확인하는 프로세스는 그림 11과 같다. 발송요청기관이 CI 일괄변환 요청 시 본인확인기관은 발송요청기관을 식별한 후 전달받은 주민등록번호를 CI로 변환

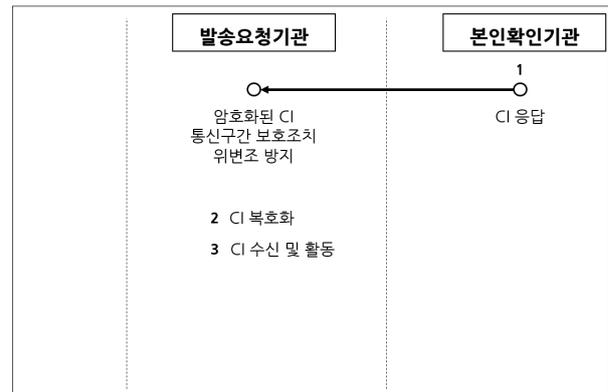


그림 11. CI일괄변환 결과 제공 프로세스
 Figure 11. Process for providing CI batch conversion results

표 4. CI일괄변환 결과 제공 처리 프로세스 및 설명
 Table 4. Process and description for delivering CI batch conversion results

순번	프로세스 명	처리 주체	설명
①	CI 응답	본인확인기관	암호화 처리한 CI를 발송요청기관으로 응답한다.
②	CI 복호화	본인확인기관	암호화 처리한 CI를 수신하고 본인확인기관과 사전에 협의한 방식으로 복호화 한다.
③	CI수신 및 활용	본인확인기관	복호화 한 CI를 저장, 모바일전자고지서비스 목적으로 수신자에게 전자문서 발송 시 활용한다.

하고 암호화한 후 발송요청기관에게 제공한다. 이때 본인확인기관은 CI 제공 시 발송요청기관과 본인확인기관 간의 전송구간 암호화를 통해 CI정보 등의 위·변조 방지 조치를 취하고 전송하는 기술기준을 제시한다. 이후 발송요청기관은 전달받은 암호화된 CI정보를 복호화하고 수신시점을 저장한다. 그리고 표 4는 CI변환 결과 확인 세부 프로세스 기준을 정의한 것이다.

4. 기관 간 정보 연동기준

CI일괄변환서비스 이용을 위해서는 본인확인기관과 발송요청기관 간에 사전에 정의된 방식으로 정보 연동이 필요하다. 제안한 방안에서 정의한 서비스 프로세스를 기반으로 안전한 CI일괄변환을 위해 본인확인기관과 발송요청기관이 준수해야할 연동 기술기준은 다음과 같다.

- ① CI변환을 위해 처리되는 수신자의 개인정보는 최소한의 항목으로 수집·처리하여야 한다.
- ② CI가 유출 등으로 기존의 CI를 사용하지 못하게 되는 경우, 기존의 CI를 대체하는 새로운 CI(CI2)를 배포할 수 있는 방안을 마련해야 한다. 두 기관 간 정보 연동을 위해서는 표 5와 같은 연동전문 상에 필수항목을 포함하는 것이 필요하다.
- ③ 본인확인기관은 CI변환을 요청한 발송요청기관이 실제 발송요청기관으로부터 발생한 정당한 요청인지 확인하는 방안을 마련해야 한다.

표 5. CI일괄변환 서비스 이용을 위한 필수항목
Table 5. Required items for using CI batch conversion service

구분	항목명	내용
발송요청기관 요청	주민등록번호	CI변환 처리를 수행할 주민등록번호
본인확인기관 응답	CI	변환처리된 CI
	CI2	변환 처리된 CI2
	CI 버전	CI버전

두 기관 간 정보 연동기준에 따라, 본인확인기관은 발송요청기관에게 CI일괄변환서비스 제공을 위한 연동은 표 6과 같은 연동규격을 정의한다. 표 6은 전자고지문 발송요청기관이 본인확인기관에게 실시간으로 수신자의 주민등록번호를 CI로 변환을 요청하기 위한 실시간 변환 처리 방식의 연동규격이다. 연계정보의 실시간 변환 처리 방식의 연동규격과 함께 다량의 연계정보를

일괄변환 처리하기 위해 필요한 일괄변환 처리 형태의 연동규격도 요구된다. 이 방식은 발송요청기관이 전자고지문 수신자의 주민등록번호를 본인확인기관에게 제공 시 단건 변환이 아닌 다량 변환요청으로써 수신자들의 각 주민등록번호 별로 부여된 일련번호를 식별하여 CI변환을 요청하도록 한 연동규격은 표 7과 같이 정의한다.

표 6. CI일괄변환서비스 실시간 변환처리 연동규격
Table 6. Connecting specification of conversion processing for CI batch conversion

구분	항목	코드	타입	길이	내용
요청	발송요청기관 코드	CP_CD	문자열	12	연계정보 변환 업무를 요청하는 발송요청기관에 대한 관리코드
	주민등록번호	SSN	문자열	13	연계정보 변환 대상 주민등록번호
응답	결과 코드	RSLT_CD	코드	가변	변환 처리 결과에 대한 응답코드
	결과 메시지	RSLT_MSG	문자열	가변	변환 처리 결과에 대한 메시지
	CI	CI	문자열	88	변환 처리된 연계정보(CI)
	CI2	CI2	문자열	88	변환 처리된 연계정보(CI2)
	CI 버전	CLVER	숫자	1	변환 처리된 CI값의 버전

표 7. CI일괄변환서비스 배치(파일) 변환 요청 처리 연동규격
Table 7. Connecting specification when processing requests for CI batch conversion of batch files

순서	항목	코드	속성	길이	설명
1	발송요청기관 코드	CP_CD	문자열	12	연계정보 변환 업무를 요청하는 발송요청기관에 대한 관리코드
2	주민등록번호	SSN	문자열	1	항목 구분자
3	결과 코드	RSLT_CD	코드	20	연계정보 변환 대상의 일련번호
4	결과 메시지	RSLT_MSG	문자열	1	항목 구분자
5	CI	CI	문자열	13	연계정보 변환 대상 주민등록번호

본인확인기관은 다 건의 주민등록번호를 기반으로 CI 일괄변환 시 각 수신자의 주민등록번호별로 일련번호를

부여하여 발송요청기관에게 제공 시 식별하도록 한다. 이때 본인확인기관이 발송요청기관에게 다 건의 CI일괄변환 처리 결과를 응답 시 처리하는 연동규격은 표 8과 같이 정의한다.

표 8. CI일괄변환서비스 배치(파일) 변환 응답 처리 연동규격
 Table 8. Connecting specification when processing response for CI batch conversion of batch files

순서	항목	코드	속성	길이	설명
1	발송요청기관 코드	CP_CD	문자열	1	연계정보 변환 업무를 요청하는 발송요청에 대한 관리코드
2	구분자	-	문자열	1	항목 구분자
3	대상일련번호	RSLQ_NO	코드	20	연계정보 변환 대상의 일련번호
4	구분자	-	문자열	1	항목 구분자
5	CI	CI	문자열	88	변환 처리된 연계정보(CI)
6	구분자	-	문자열	1	항목 구분자
7	CI2	CI2	문자열	88	변환 처리된 연계정보(CI2)
8	구분자	-	문자열	1	항목 구분자
9	CI 버전	CL_VER	문자열	1	변환 처리된 CI값의 버전

5. 암호화 기준

CI일괄변환서비스 제공 시 데이터 보호와 정확하고 안전하게 처리하기 위해 발송요청기관과 본인확인기관 간 개인정보는 본 연구에서 제안한 연동기준에 따라 암호화 되어야 하며, 위조·변조·해킹 시도 등 각종 위협으로부터 안전하게 보호하도록 암호화 기술기준을 제시한다.

- ① 개인정보는 안전한 대칭키 암호화 알고리즘을 통해 암호화 되어야 한다.
- ② 암호화키는 최대 2년 내에 주기적으로 갱신되어야 하며, 키 교환은 안전한 방법으로 이루어져야 한다.
- ③ 데이터 위조나 변조 되었을 경우 이를 탐지할 수 있도록 메시지검증코드 등을 사용하여 무결성을 검증해야 한다. 또한 메시지가 위조나 변조 되었을 경우 위조나 변조된 데이터를 사용하여서는 아니 된다.

안전한 CI일괄변환서비스 이용을 위해서는, 두 기관 간 연동 데이터는 표준을 따르는 안전한 알고리즘을 통해 암호화하는 것이 필요하다. 이때 적용하는 암호 알고리즘은 시간이 지남에 따라 달라질 수 있으므로, 암호화 적용 시, 국내·외 암호 관련 기관 [10]에서 제시하는 최신 기술을 적용하는 것이 요구된다. 그리고 안전한 CI일괄변환서비스 활용을 위해, 네트워크를 활용하여 암호화키 교환 시 표준을 따르는 안전한 공개키 암호화 알고리즘을 사용하여야 한다.

모바일 전자고지서비스에서 두 기관 간 안전한 CI일괄변환서비스 활용을 위해, 데이터 위조나 변조되었을 경우 이를 탐지할 수 있도록 메시지검증코드 등을 사용하여 무결성을 검증해야 한다. 송·수신 기관간의 데이터 무결성 검증 그림 12와 같이 수행한다. 이때, 무결성 검증을 위해 사용되는 해시 알고리즘은 표준[10]을 따르는 안전한 알고리즘을 사용하여야 한다. 두 기관 간 안전한 서비스 제공을 위해 데이터 암호화를 위한 암호 알고리즘의 보안강도는 키 길이와 관련이 있다. 즉, 키 길이가 길수록 해독 시간이 많이 소요 되고 보안 강도가 높아진다고 볼 수 있다 이러한 암호 알고리즘에 대한 적절한 키 크기를 선택할 때에는 알고리즘의 보안강도와 해당 알고리즘의 안전성 유지기간 및 보호하고자 하는 데이터의 예상 보안 수명을 고려하여야 한다. 따라서 본 연구에서 안전한 CI일괄변환서비스 활용을 위해, NIST에서 권고하는 키 길이(보안강도) 권고안을 바탕으로 2031년 이후에도 안전하게 알고리즘을 사용할 수 있도록 키 길이에 대한 기준을 정의하였다. 표 9는 CI일괄변환서비스의 안전한 사용을 위한 암호화키 길이에 대한 기술기준을 정의한 것이다.

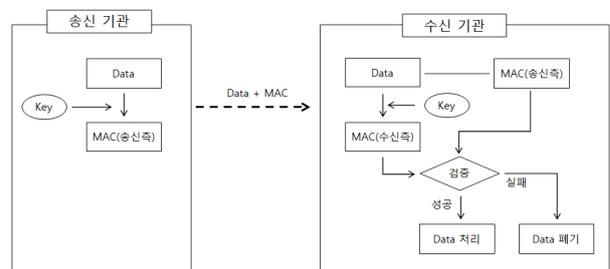


그림 12. 데이터 무결성 검증을 위한 MAC 처리 과정
 Figure 12. MAC information adding processing process for data integrity verification

표 9. CI일괄변환서비스의 안전한 사용을 위한 키 길이 기준
Table 9. Encryption key length for secure use of CI batch conversion services

대칭키 암호알고리즘 키 길이	공개키 암호 알고리즘 키 길이	해시함수 (보안강도)
128비트 이상	3,072비트 이상 (단, 타원곡선 알고리즘의 경우 128비트 이상)	128비트 이상

6. 통신구간 보호조치 기준

안전한 CI일괄변환서비스 활용을 위해, 네트워크를 활용하여 본인확인기관과 발송요청기관 간 연동 데이터 송·수신 시, 불법적인 접근 및 침해 사고방지를 위해 통신구간에 대한 연동기술 기준은 다음과 같이 정의한다.

- ① 접근통제를 적용하여 허가받지 않은 접근에 대하여 차단할 수 있어야 한다.
- ② 통신구간에 전용선을 사용하거나 SSL/TLS 1.2 이상을 적용하여야 한다.

7. 개인정보 보관기준

기관 간 CI일괄변환서비스 목적으로 수신자의 개인정보 연동 시 관련 법령에 의거 목적이 달성된 개인정보(CI 등)는 복구 또는 재생되지 않는 방법으로 지체 없이 파기하여야 하며, 법령 등에 따라 보존해야 하는 경우 해당 개인정보를 다른 개인정보와 분리하여서 저장 관리하도록 기술기준을 제시한다. 정보주체가 자신의 개인정보에 대한 열람·정정·삭제·처리정지를 개인정보처리자에게 요구할 경우 개인정보처리자는 정보주체의 요구에 응하도록 기술기준을 제시한다. 개인정보보호법에 근거하여 안전한 CI활용을 위해 CI일괄변환서비스 발송요청기관이 준수해야 할 개인정보 보관기준은 다음과 정의한다.

- ① 발송요청기관은 모바일전자고지서비스 이용 목적으로 변환한 CI를 모바일전자고지서비스 이용 목적 외 다른 목적으로 사용할 수 없다.
- ② 정보주체가 CI변환에 대한 처리내역에 대한 열람, 정정·삭제, 처리정지를 요구 시, 발송요청기관은 개인정보 보호법에 따라 정보주체가 개인정보를 열람할 수 있도록 하는 등의 조치를 하여야 한다.
- ③ 발송요청기관은 모바일전자고지서비스 이용 목적

으로 CI 등 개인정보를 보관하는 경우, 다른 서비스의 개인정보와 물리적 또는 논리적으로 분리하여 암호화 하여 보관하여야 한다. 이때 CI 등 개인정보는 보관기관 경과 시, 복구 또는 재생할 수 없는 방법으로 지체 없이 파기하여야 한다.

그리고 안전한 CI활용을 위해, 본인확인기관이 준수해야 할 개인정보 보관기준은 다음과 같이 제시한다.

- ① 본인확인기관은 CI일괄변환서비스 목적으로 처리한 개인정보를 다른 목적으로 사용할 수 없다.
- ② 본인확인기관은 CI일괄변환서비스 목적으로 처리한 개인정보는 즉각 파기하여야 한다. 단, 발송요청기관이 정보주체의 개인정보열람 및 제공 목적으로 처리내역을 요청 할 시, 처리내역 제공을 목적으로 일부 항목을 1년간 보관하여야 한다. (이때, CI정보는 암호화 하여 보관하여야 한다.) 저장하는 일부 항목은 CI 변환일시, 발송요청기관명 등 발송요청기관과 관련된 정보, CI 등이다.
- ③ 본인확인기관이 불가피한 사정으로 CI 보관이 불가능한 경우, 업무처리 기록을 보관하여야 한다. 기록하는 사항에는 CI 변환일시, 발송요청기관명 등 발송요청기관과 관련된 정보, 변환 처리된 연계정보 건수, 작업방법, 본인확인기관의 연계정보 변환업무 작업자 명, 발송요청기관의 연계정보 변환업무 작업자 명, 본인확인기관이 처리내역 제공을 목적으로 개인정보를 보관하는 경우, 다른 서비스의 개인정보와 물리적 또는 논리적으로 분리하여 보관하여야 하며, 보관기간 경과 시, 복구 또는 재생할 수 없는 방법으로 지체 없이 파기하여야 하도록 기술기준을 정의한다.

V. 결 론

본 논문에서는 민간기관 등이 종이고지서를 모바일 기기를 활용한 전자고지서로 발송하기 위해 필요한 기술기준을 제안한다. 제안한 기술기준은 민간기관 등이 본인확인기관에게 모바일 전자고지문 수신자를 식별하기 위해 사용하는 연계정보의 일괄변환을 위한 기술기준이다. 전자고지문 발송요청기관은 관련 법령에 의해 수신자의 주민등록번호는 동의를 받아 저장하고 있으나 온라인 서비스 가입 여부를 확인하기 위한 연계정보는 수집하고 있지 않은 문제점이 있다. 이를 해결하기

위해 발송요청기관은 본인확인기관에게 수신자의 주민등록번호를 제공하여 연계정보로 일괄 변환하는 것이 필요하다. 이후 발송요청기관은 공인전자문서중계사업자에게 연계정보와 전자고지문을 제공하여 온라인 서비스 가입자를 식별한 후 해당 수신자에게 전자고지문을 발송한다. 이때 발송요청기관과 본인확인기관은 수신자의 주민등록번호와 연계정보에 대해 사전에 제3자 제공 동의를 직접적으로 받을 수 없는 법 위반이 발생하게 된다. 이를 ICT 규제샌드박스 제도를 통해 수신자의 사전 동의가 아닌 사후 동의 개념으로 연계정보를 일괄변환하고 공인전자문서중계사업자에 가입되어 있는 수신자를 식별한 후 모바일 전자고지문을 발송하도록 허용하였다. 그동안 모바일 전자고지서비스는 종이 기반의 우편 고지서비스에 대비 저탄소, 비용절감, 개인정보 노출방지, 환경 보호 등으로 인해 급속하게 활성화되고 있다. 하지만, 모바일 전자고지서비스의 활성화 이면에는 온라인상의 주민등록번호라고 불리는 연계정보 고지문 수신자가 미처 인지하지 못한 상황에서 도처에 제공되고 있다. 이렇게 제공받은 연계정보에 대해 보호 기준이 존재하지 않으며 연계정보 일괄변환을 위한 관련 기술기준도 존재하지 않는 상황이다. 따라서 본 연구에서는 모바일 전자고지문 발송요청기관과 본인확인기관간의 연계정보의 일괄변환 처리를 위한 기술기준을 제안한다. 제안한 기술기준안에는 연계정보 일괄변환 세부 프로세스, 서비스 흐름도, 개인정보 흐름도, 그리고 연동규격을 제시하고, 각 세부 프로세스에 대한 상세 정의를 바탕으로 안전한 연계정보 일괄변환서비스가 이루어 질 수 있도록 데이터 암호화, 전송구간 암호화, 정보 처리 및 관리 방안 등을 제안한다. 제안한 기술기준을 민간기관 등이 모바일 전자고지서비스 이용 시 적용함으로써 표준화된 정보 연동에 따른 안전하고 효율적인 서비스 관리가 가능할 것이다. 향후 연구에서는 민간기관과 공인전자문서중계사업자 간에 공유하고 있는 전자고지문 수신자의 연계정보에 대한 안전한 활용과 보호를 위한 기술기준을 개발하고자 한다. 최근까지도 모바일 전자고지문을 활용함으로써 발생하는 사회적인 편익에만 치중하고 있으나 그 이면에서는 수신자의 동의 여부와 관련 없이 연계정보가 무분별하게 공공·행정기관 그리고 민간기관 등에게 제공되고 있는 것이 사실이다. 실제 얼마나 많은 연계정보가 제공되고 있는지에 대한 실태 파악도 필요할 것이다. 현재 본인

확인서비스를 통해 온라인 서비스 이용자가 직접 동의한 사실에 대해서는 e-Privacy 사이트에서 연계정보 제공 현황을 파악할 수 있으나 모바일 고지서비스 목적으로 일괄 변환된 연계정보에 대해서는 열람하거나 제공 중지 등을 요청할 수 없는 한계점을 가지고 있다. 이러한 한계점들은 연계정보에 대한 법적인 정의를 수립하고, 활용 시 처리 방안을 입법화하는 것이 요구된다. 이후 연계정보 일괄변환 가이드라인 등을 제시함으로써 연계정보를 사용하는 각 기관들에게 안전한 활용에 대해 안내할 필요가 있다.

References

- [1] J. B. Kim, "A Study on Establishment of Connecting Information Conversion Criteria for Mobile Electronic Notification Service of Private Institutions", *The Journal of the Convergence on Culture Technology*, vol. 7, no. 4, pp. 735-743, 2021.
- [2] J. B. Kim, "A Study on the Actual Use of Mobile Electronic Notification Service", *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 21, no. 5, pp. 167-180, 2021.
- [3] J. B. Kim, "A Study on the Securing Technological Safety of Mobile Electronic Notification Service in Public and Administrative Agencies", *Journal of the Institute of Internet, Broadcasting and Communication*, vol. 20, no. 4, pp. 7-16, 2020.
- [4] 김인섭, 유상이, "물류로봇 동향과 우편물류로봇 도입에 관한 소고", *우정정보*, vol. 122, no. 3, pp. 15-44, 2020.
- [5] 양광완, 진경식, 홍희경, 이석준, "법적 효력을 갖춘 전자문서 기반의 민원·행정 디지털 트랜스포메이션", *한국인터넷프라이즈아키텍처학회*, vol. 18, no. 1, pp. 64-74, 2021.
- [6] 김태호, 정송이, "지방세 고지서 송달제도 개선방안", *한국지방세연구원*, 정책과제 2015-14, 2015.
- [7] <https://zdnet.co.kr/view/?no=20200625154908>
- [8] <http://m.joseilbo.com/news/view.htm?newsid=382206>
- [9] 전자문서 및 전자거래 기본법, <https://www.law.go.kr>
- [10] 암호 알고리즘 및 키 길이 안내서, 한국인터넷진흥원, 2018.

※ 이 논문은 2021년도 산업통상자원부 규제 샌드박스융합신제품인증기술개발사업의 지원(20016800)과 과학기술정보통신부와 한국연구재단 보조금에 의해 지원된 연구임(NRF-2020R1F1A106890011).