기록관리시스템 표준

NAK 33:2013(v1.1)

National Archives Standard

전자기록물 온라인 전송을 위한 기술 규격(v1.1)

Technical Specification for
Online Transmission of Digital Records(v1.1)

Version 1.1

국가기록원
National Archives of Korea

2010년 12월 30일 제정
2013년 12월 30일 개정

○ 제·개정자 : 안전행정부 국가기록원장
○ 제 정 일 : 2010년 12월 30일(행정안전부 고시 제2010-78호)
○ 개 정 일 : 2013년 12월 30일(안전행정부 고시 제2013-53호)
○ 심　　의 : 국가기록관리위원회, 표준전문위원회
○ 원안 작성 : 강윤정(국가기록원 전산주사보)
○ 개정안 작성 : 구명회(국가기록원 전산주사)
○ 검　　토 :
• 김현정(국가기록원 전산사무관)
• 이윤경(국가기록원 기록연구사)
• 이젬마(국가기록원 사서사무관)
○ 관　　리 :
• 국가기록원 표준협력과
○ 자　　문 :
•

(1) 이 표준에 대한 의견 또는 질문은 아래 전화로 연락하거나 홈페이지를 이용하여 주십시오.

• 표준열람: 국가기록원(http://www.archives.go.kr)→기록관리안내 →기록관리표준→표준화현황
• 안전행정부 국가기록원 기록정보서비스부 기록정보화과(042-481-6324)
기록정책부 표준협력과(042-481-6246)

목 차

머리말

이 표준은 전자기록물의 온라인 전송을 위한 송·수신 전송 기술규격을 규정하기 위하여 제정되었다.

이 표준은 다음과 같이 구성하였다. 제1절부터 제3절에서는 표준의 적용범위와 인용표준 제시 및 용어를 정의하였다. 제4절에서는 전자기록물 송·수신 모듈의 기능 요구사항을 기술하였으며, 제5절에서는 업무시스템과의 연계 인터페이스, 제6절에서는 송·수신 프로토콜을 정의하였다.

이 표준에 따라 '전자기록물 온라인 전송 소프트웨어(이하 '전송소프트웨어'로 한다)'를 구축할 경우 대용량 전자기록물의 온라인 전송을 효율적으로 수행할 수 있을 것으로 기대된다.

이번 개정안에서는 업무시스템의 변경을 최소화하고자 각 시스템간 데이터 전송을 위한 전 처리 모듈을 개발하여 구 '전송목록XML'을 신규 '전송목록XML' 형식으로 변환하는 신규 기술규격을 추가하였다.

또한 데이터 모니터링 기능을 강화할 수 있도록 로그파일 작성 및 추가기능을 적용하여 기존 업무시스템의 변경을 최소화하면서 업무의 편의성을 보장할 수 있도록 하였다.

이 표준은 기록관리 표준전문위원회 및 국가기록관리위원회 심의를 거쳐 제정되었으며 국가기록원이 유지·관리한다. 이 표준은 관련 법령의 개정, 관계 기관 및 이해 당사자의 요청 등 개정 사유가 발생할 경우 그 필요성 및 타당성을 검토한 후 개정안을 마련하고 전문가 검토 및 의견수렴 절차를 거쳐 개정을 추진한다.

전자기록물 온라인 전송을 위한 기술규격

1 적용범위

이 표준은 「공공기록물 관리에 관한 법률」에 따른 각급 공공기관이 구축, 운영하고 있는 전자기록물 생산·관리시스템 간에 기록물을 온라인으로 전송하기 위한 기술규격을 제시하며 각 시스템의 전송요청 및 접수요청에 관한 인터페이스의 구현에 적용된다.

전자기록물의 이관·인수 기능을 수행하는 전자기록생산시스템, 기록관리시스템, 영구기록관리시스템 등 업무시스템은 이 표준의 제5절 업무시스템과의 연계 인터페이스를 준수하여야 하며, 대용량 기록물 파일을 전송하는 대용량 송·수신 소프트웨어는 이 표준을 모두 준수하여 개발, 관리되어야 한다.

2 적용근거

2.1 법적 근거

이 표준의 구체적인 법적 근거는 다음과 같다.

- 「공공기록물 관리에 관한 법률」 제20조(전자기록물의 관리)
- 「공공기록물 관리에 관한 법률」 시행령 제32조(기록물의 이관)
- 「공공기록물 관리에 관한 법률」 시행령 제40조(기록관 및 특수기록관의 소관 기록물 이관)

2.2 인용표준

이 표준은 다음의 표준을 참조하여 관련 조항을 구성하였다.

- KS X ISO 15489-1:2007, 문헌정보-기록관리 - 제1부 : 일반
- KS X ISO/TR 15489-2:2007, 문헌정보-기록관리 - 제1부 : 지침

2.3 다른 표준과의 연계

- NAK/TS 1-1:2012(v1.2) 기록관리시스템 데이터연계 기술규격-제1부: 업무관리시스템과의 연계(v1.2)
- NAK/TS 1-2:2008(v1.0) 기록관리시스템과 영구기록관리시스템간 데이터 연계규격(v1.0)

3 용어정의

이 표준의 목적을 위하여 다음의 용어와 정의를 적용한다.

3.1 업무시스템

전자기록물을 생산하고 관리하는 정보시스템. 전자기록물 전송소프트웨어와 연계될 수 있는 업무관리시스템, 전자문서시스템, 자료관시스템, 기록관리시스템, 영구기록관리시스템 등이 포함된다.

3.2 송・수신 모듈

송신모듈과 수신모듈을 통칭하는 용어

비고 송신모듈은 업무시스템으로부터 전자기록물 전송요청을 수신하여 전자기록물을 수신모듈로 전송하는 기능을 수행하는 모듈이고, 수신모듈은 송신모듈이 전송한 전자기록물을 수신하여, 업무시스템에 접수를 요청하는 기능을 수행하는 모듈을 의미한다.

3.3 요청(request)

송신모듈이 수신모듈에게 전자기록물을 전송하기 위해 필요한 메시지를 전송하는 것

3.4 응답(response)

송신모듈의 요청에 대해 응답메시지를 반환하는 것

3.5 전송/접수 요청 인터페이스

업무시스템이 전자기록물 송·수신모듈에게 전송/접수 동작을 개시할 수 있도록 명령을 지시하거나 처리결과를 전달받을 수 있는 인터페이스

3.6 전송목록파일

전송할 전자기록물파일 목록 및 파일정보를 포함한 파일

3.7 다중세션 전송(multi session transfer)

하나 또는 다수의 송신모듈에서 수신모듈로 파일을 전송할 때 여러 세션을 이용해 병렬로 전송하는 기능

3.8 다중파일 전송(Multi file transfer)

송신모듈에서 수신모듈로 파일을 전송할 때 생성된 하나의 세션을 유지하면서 순차적으로 전송하는 기능

3.9 메시지 무결성(Message integrity)

전송 도중에 메시지의 내용이 부당하게 변경되었는지를 확인해 주는 기능
[한국정보통신기술협회 정보통신용어사전]

비고 무결성은 네트워크를 통해 송·수신되거나 정보 시스템에 보관되어 있는 정보가 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보장하는 성질이다.

3.10 수신이력 시각정보 생성

수신 완료시 전송목록파일에 대한 시점확인 토큰을 생성하는 것

비고 시점확인 토큰(TST, Time Stamp Token, RFC 3161 참조)은 특정시간에 해당데이터가 존재했음을 보장하고, 시점확인토큰은 시점확인시스템(TSA, Time Stamp Authority)이 발급한다.

3.11 전송 제어 프로토콜/인터넷 프로토콜(Transmission control protocol/ Internet protocol, TCP/IP)

컴퓨터 간의 통신을 위해 미국 국방성에서 개발한 통신 프로토콜로, TCP와 IP를 조합한 것. TCP/IP는 현재 인터넷에서 사용되는 통신 프로토콜로 통신 프로토콜이 통일됨에 따라 세계 어느 지역의 어떤 기종과도 정보 교환이 가

능하게 되었다. RFC(Request for Comments) 행태로 공개되고 있고 유닉스에서는 표준 프로토콜로 설정되어 있으며 거의 모든 운영 체계에서 구현되고 있으므로 널리 보급되어 있다.
[한국정보통신기술협회 정보통신용어사전]

3.12 무손실 압축알고리즘(Lossless compression algorithm)

압축된 데이터를 다시 복원했을 때 압축되기 이전의 원래 데이터와 모든 비트가 일치하는 압축 알고리즘
[한국정보통신기술협회 정보통신용어사전]

3.13 SSL(Secure Sockets Layer)

데이터를 송수신하는 두 컴퓨터 사이, 종단 간 즉 TCP/IP 계층과 애플리케이션 계층(HTTP, TELNET, FTP 등) 사이에 위치하여 인증, 암호화, 무결성을 보장하는 업계 표준 프로토콜

3.14 TLS(Transport Layer Security)

현재 널리 사용되고 있는 SSL(Security Sockets Layer)을 대체할 차세대 안전 통신 규약. SSL에 비해 강력한 암호화를 실현할 수 있고 폭이 넓은 망의 통신 규약에 대응되어 있는 점에서 주목을 끌고 있다. 암호화에는 3개의 다른 데이터 암호화 표준(DES) 키를 사용한 트리플(triple) DES 암호화 기술이 응용되고 있다.
[한국정보통신기술협회 정보통신용어사전]

3.15 SHA(Secure Hash Algorithm)

미국 국립표준기술연구소인 NIST(National Institute of Standards and Technology)가 표준으로 채택한 암호 해시 함수(Cryptographic Hash Function). SHA에는 현재까지 6개 해시 함수(SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)가 있다.
[한국정보통신기술협회 정보통신용어사전] 참조하여 개작

3.16 SignedData

디지털 서명을 위한 구문 표현. 서명값 및 서명자의 인증서 정보, 그리고 서명한 원본 등의 정보를 포함할 수 있다.

비고 PKCS#7은 디지털 서명이나 디지털 봉투와 같은 암호 응용에 대한 결과가 가질 수 있는 일반적인 구문 표현에 대해 설명한다.

3.17 소켓(socket)

어떤 통신망의 특정 노드상의 특정 서비스를 식별하는 식별자. 소켓은 노드 주소와 서비스를 식별하는 포트 번호로 구성된다.
[한국정보통신기술협회 정보통신용어사전]

3.18 파일블록(File block)

1개의 단위로 취급하는 단어 또는 레코드나 문자들의 집합

비고 컴퓨터에서 파일의 최소의 입출력 단위를 의미한다.
[한국정보통신기술협회 정보통신용어사전]

3.19 오픈소스(Open source)

소스코드나 표준을 공개하여 자유로운 개작, 재배포 등을 허용하면서도 저작권자의 권익을 보호하고, 공동 개발을 장려하는 소프트업계의 뚜렷한 하나의 제도화된 흐름
[한국정보통신기술협회 정보통신용어사전]

3.20 DN(distinguished name, 식별이름)

ITU-T X.500 디렉터리에서 정하는 이름 형식. X.500 디렉터리에서 개체를 인식하기 위해 국가, 지역, 기관, 이름 등 개체의 속성으로 구성된 것으로, 디렉터리 정보 트리(DIT)의 경로를 나타내는 통신 개체의 유일한 이름을 부여하는 구조를 제공하며, 인증서 발급자 및 인증서 소유자를 확인하기 위해 사용된다.
[한국정보통신기술협회 정보통신용어사전]

3.21 접근토큰(Access token)

로그온 수행 시 필요한 보안 정보가 들어 있는 일종의 객체. 로그온 할 때 만들어지며 프로세스마다 하나의 토큰 사본이 필요한 것으로, 사용자, 사용자 그룹 및 사용자의 특권을 식별하며, 시스템에서 보안 객체의 접근 및 시스템 운용 제한을 위해 사용된다.
[한국정보통신기술협회 정보통신용어사전]

3.22 ASN.1(Abstract Syntax Notation One, 추상 구문 기법 1)

OSI 기본 참조 모델의 응용 계층에서 취급하는 다양한 종류의 데이터를 표현하기 위하여 배커스 나우어 형식(BNF)을 기반으로 개발한 표기법
[한국정보통신기술협회 정보통신용어사전]

3.23 IV(Initialization vector, 초기화 벡터)

대칭적 암호화 알고리즘의 초기화에 쓰이는 임의의 2진 데이터
[한국정보통신기술협회 정보통신용어사전]

3.24 SEED(시드 블록 암호 알고리즘)

민간 부분인 인터넷, 전자 상거래, 무선 통신 등에서 공개 시에 민감한 영향을 미칠 수 있는 정보와 개인 프라이버시 등을 보호하기 위하여 개발된, 블록 단위로 메시지를 처리하는 대칭키 블록 암호 알고리즘
[한국정보통신기술협회 정보통신용어사전]

4 전자기록물 송·수신 모듈의 기능

4.1 송·수신 절차 개요

전자기록물 송신모듈과 수신모듈 간에 이루어지는 전송 절차의 개요는 **그림 1**과 같다. **그림 1**은 업무시스템과 송·수신모듈간의 기본적인 업무절차를 기술한 것으로 세부적인 동작절차 및 오류 처리는 **그림 18, 그림 19, 그림 20, 그림 21, 그림 22**를 참조한다.

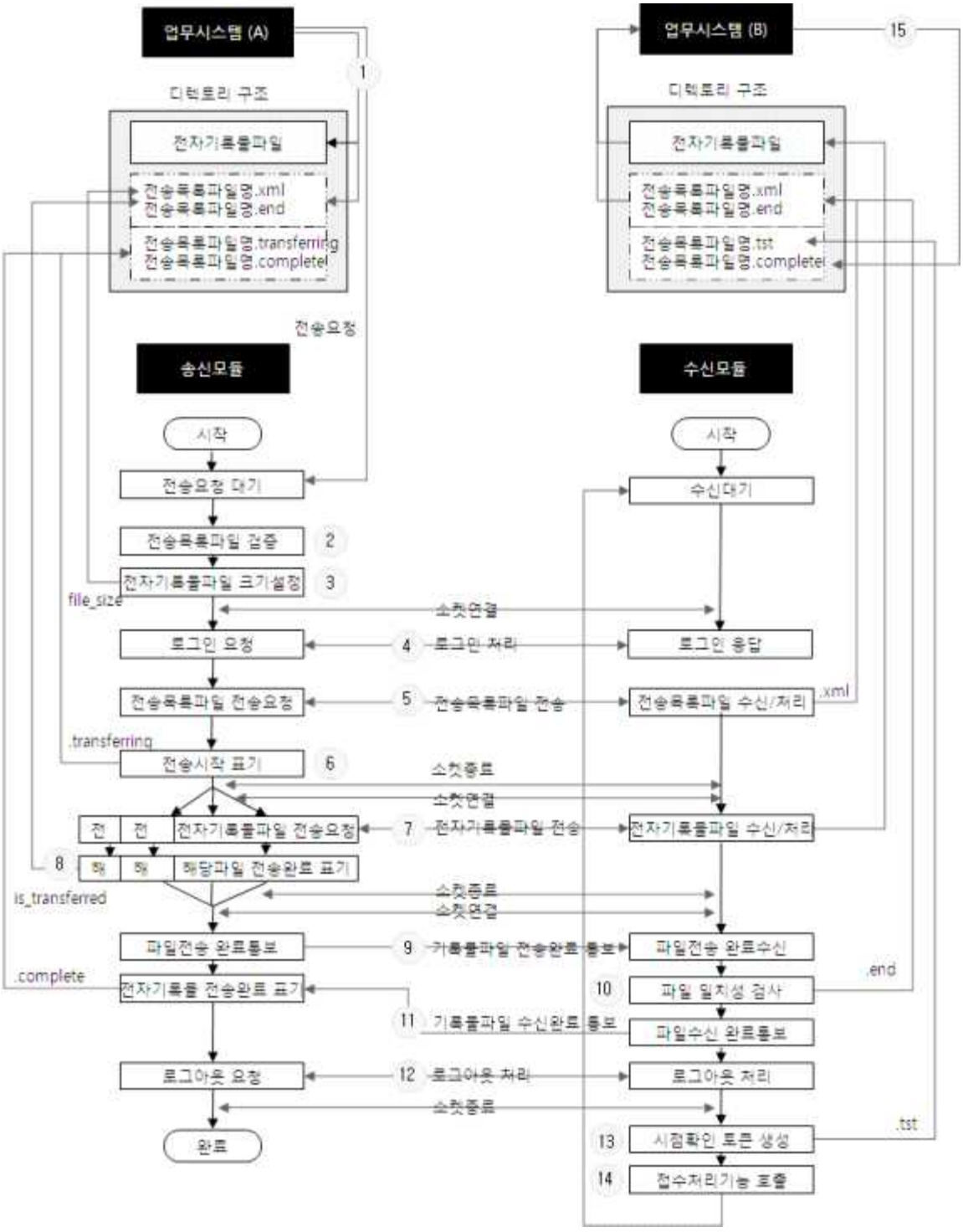

그림 1 - 전자기록물 온라인 전송절차 개념도

① 업무시스템 전자기록물 전송요청

・업무시스템은 전송할 전자기록물파일 및 전송목록파일을 지정된 디렉토리에

생성한다.
- 전송목록파일을 생성하면 송신모듈에 전자기록물 전송을 요청한다.
- 세부 기술규격은 '5. 업무시스템과의 연계 인터페이스'를 참고한다.

② 전송목록파일 검증
- 송신모듈은 업무시스템의 전송요청에 따라 전송목록파일의 규격 및 전자기록물파일을 검사한 후 검사결과를 업무시스템으로 반환한다.
- 전송목록파일 검증 시 오류가 발생하면 해당 오류코드를 반환하고 전송작업을 중단한다. 관련 오류 내역은 '6.4.2 오류내역을 위한 로그포맷'에 정의된 형식을 준용하며 파일로 기록되어야 한다.
- 세부 기술규격은 '5.3 업무시스템과 송·수신모듈 간 인터페이스'를 참고한다.

③ 전자기록물파일 크기 설정
- 송신모듈은 업무시스템에서 생성한 전송목록파일 내의 파일크기를 설정한다.
- 세부 기술규격은 '5.2.1 전송목록파일 구조'를 참고한다.

④ 로그인 처리
- 송·수신모듈은 '접근토큰'을 공유한 후, 사용자 인증을 통해 로그인을 수행한다. 로그인 후 인증된 접근토큰은 로그아웃 시점까지 로그인 수행여부를 보증하는 용도로 사용된다.
- 로그인과 로그아웃 단위는 전송목록파일 단위로 이루어진다. 그러므로 하나의 전송목록파일을 보내기 위해 로그인을 수행하고, 전송목록파일에 기술된 전자기록물파일을 모두 전송하고 전송완료 통보를 수행한 이후 로그아웃한다.
- 로그인에 대한 세부 기술규격은 '6.3.4.1 접근토큰 요청(OP0001)', '6.3.4.2 접근토큰 응답(OP0002)', '6.3.4.3 로그인 요청(OP0003)', 그리고 '6.3.4.4 로그인 응답(OP0004)'을 참고한다.

⑤ 전송목록파일 전송
- 송신모듈은 전송목록파일 전송요청메시지를 생성하여 수신모듈에 전송한다.
- 수신모듈은 전송목록파일을 지정된 디렉토리에 저장한다.

- 전송목록파일관련 세부 기술규격은 '5.1 디렉토리 구성'에서 설명한다.
- 세부 기술규격은 '5.1 디렉토리 구성', '6.3.4.7 전송통지 요청(OP0011)', '6.3.4.8 전송통지 응답(OP0012)', '6.3.4.9 파일전송 요청(OP0013)', '6.3.4.10 파일전송 응답(OP0014)'을 참고한다.

⑥ 전송시작표기

- 송신모듈은 해당 전송목록파일에 대해 전송진행을 표기한다.
- 세부 기술규격은 '5.2.2 전송목록파일 관리방안'을 참고한다.

⑦ 전자기록물파일 전송

- 송신모듈은 전자기록물파일을 수신모듈에 전송한다.
- 수신모듈은 수신한 전자기록물파일을 지정된 디렉토리에 저장한 후 처리결과에 대한 응답메시지를 전달한다.
- 송신모듈은 전자기록물파일을 다중세션을 통해 병렬로 전송할 수 있어야 하고, 수신모듈은 병렬로 전송된 파일을 처리할 수 있어야 한다.
- 세부 기술규격은 '5.1 디렉토리 구성', '6.3.4.7 전송통지 요청(OP0011)', '6.3.4.8 전송통지 응답(OP0012)', '6.3.4.9 파일전송 요청(OP0013)', '6.3.4.10 파일전송 응답(OP0014)'을 참고한다.

⑧ 해당파일 전송완료 표기

- 송신모듈은 전송 완료된 해당 전자기록물파일에 대해 전송목록파일에 전송완료를 설정한다.
- 세부 기술규격은 '5.2 전송목록파일'에서 설명한다.

⑨ 기록물파일 전송완료 통보

- 송신모듈은 전송목록파일에 기술된 모든 전자기록물파일을 전송완료 했음을 통보한다.
- 전자기록물 전송완료 통보에 대한 세부 기술규격은 '6.3.4.7 전송통지 요청(OP0011)' 메시지 규격을 참조한다.

⑩ 파일 일치성 검사

- 수신모듈은 수신 완료한 전자기록물파일에 대해 파일 일치성을 검사한다.
- 수신모듈은 파일 일치성이 보장된 경우에 한해 지정된 디렉토리에 .end파일을 생성한다.

- 디렉토리 및 파일에 대한 세부 기술규격은 '5.1 디렉토리 구성', '5.2.2 전송목록파일 관리방안'에서 설명한다.
- 파일 일치성 검사는 '4.2.6 파일 일치성 보장'을 참조한다.

⑪ 기록물파일 수신완료 통보

- 수신모듈은 파일 일치성 검사 결과를 응답메시지로 전달한다.
- 송신모듈은 수신모듈로부터 성공적인 파일수신 완료통보를 수신하면 절차 ⑥에서 생성한 전송시작 표기 파일을 삭제하고 해당 전송목록파일에 대해 전송완료를 표기한다.
- 송신모듈은 수신모듈로부터 오류메시지를 수신하면 전자기록물파일 전송완료 표기를 수행하지 않고 해당 기록물을 오류 처리하여야 한다.
- 송신 측 업무시스템은 해당 전송목록파일에 대한 '.complete' 파일의 존재여부로 성공적인 전송완료 여부를 확인할 수 있다.
- 전송완료 표기관련 세부 기술규격은 '5.1 디렉토리 구성', '5.2.2 전송목록파일 관리방안'에서 설명한다.
- 전자기록물 수신완료 통보에 대한 세부 기술규격은 '6.3.4.8 전송통지 응답(OP0012)' 메시지 규격을 참조한다.

⑫ 로그아웃

- 송·수신모듈은 로그아웃을 수행한다. 로그아웃을 수행하면 송·수신모듈 간 공유한 접근토큰은 더 이상 사용될 수 없다.
- 로그아웃에 대한 세부 기술규격은 '6.3.4.5 로그아웃 요청(OP0005)', '6.3.4.6 로그아웃 응답(OP0006)'에서 설명한다.

⑬ 시점확인 토큰생성

- 수신모듈은 전자기록물 수신완료 시 전자기록물 정보에 대한 시점정보 및 부인방지 정보 생성을 위해 수신한 전송목록파일에 대한 시점확인 토큰을 생성한다.
- 세부 기술규격은 '5.2.2. 전송목록파일 관리방안', '6.2.5 [P4] 시점확인토큰 생성 세부 흐름도'를 참조한다.

⑭ 접수처리 기능 호출

- 수신모듈은 업무시스템에서 제공하는 '접수처리기능'을 실행할 수 있도록 한다.

⑮ 업무시스템 접수처리

- 업무시스템은 수신이 완료된 전자기록물파일을 접수 처리한다. 접수처리가 완료되면 업무시스템은 '.complete' 파일을 생성한다.
- 세부 기술규격은 '5.1 디렉토리 구성', '5.2.2 전송목록파일 관리방안'에서 설명한다.

송신모듈 및 수신모듈은 해당 전송목록파일 및 전자기록물파일 전송 중 발생한 오류내역을 '5.2.2. 전송목록파일 관리방안'에서 정의한 '.error' 파일에 기술하여야 한다. 오류형식은 '6.4.2. 오류내역을 위한 로그포맷'을 참조한다.

4.2 기능 요구사항

전송소프트웨어는 표 1에서 기술한 기능을 반드시 지원하여야 한다.

표 1 - 전송소프트웨어 주요기능

기능명	기능설명	필수/선택
전송/접수 요청 인터페이스	전자기록물파일 송신모듈에게 전송을 개시하거나 수신모듈이 업무관리시스템에게 인수 동작을 개시할 수 있도록 접수요청하고 처리결과를 전달받을 수 있는 인터페이스	필수
파일전송	파일을 파일블록 단위로 전송하고 수신측에 동일한 파일이름으로 저장하는 기능	필수
다중세션 전송	하나 또는 다수의 송신모듈에서 여러 세션을 이용하여 전자기록물파일을 병렬로 전송하는 기능	필수
다중파일 전송	생성된 하나의 세션을 유지하여 다수의 전자기록물 파일들을 순차적으로 전송	필수
데이터 압축	전송하기 위한 세분화된 파일블록의 전송정보를 압축하는 기능	필수
전송파일 암호화	전송정보를 SSL/TLS기반으로 암호화하는 기능	필수
재전송	전송할 파일 또는 블록을 다시 전송하는 기능	필수
이어보내기	전송한 파일 또는 파일의 블록 이후의 정보를 이어서 전송하는 기능	필수
무결성 정보 생성	전송 대상 메시지에 대한 위변조 여부를 보장하기 위하여 해쉬값을 생성, 검증하는 기능	필수
파일 일치성 검사	전송 대상 파일에 대해, 파일명, 파일확장자 그리고 파일크기가 수신한 파일과 일치함을 검사하는 기능	필수

수신이력 시각정보 생성	수신이력에 대한 시점확인 토큰을 생성하는 기능	필수
접속관리	수신모듈로 접속 실패 시 접속 재시도 횟수를 관리하는 기능	필수
사용자 인증	송·수신 모듈간의 상호인증 및 인가절차 기능	필수
로그기능	파일의 전송여부, 전송정보, 시스템 정상작동 여부를 확인 할 수 있는 정보를 파일로 기록하는 기능	필수

4.2.1 파일전송

파일전송은 TCP/IP Socket방식을 이용하여 전송하고, 수신 측에서는 동일한 파일이름으로 저장되어야 한다. 또한 전자기록물파일을 효율적으로 전송할 수 있도록 **그림 2**와 같이 전자기록물을 일정 크기의 파일블록 단위로 읽어서 전송한다.

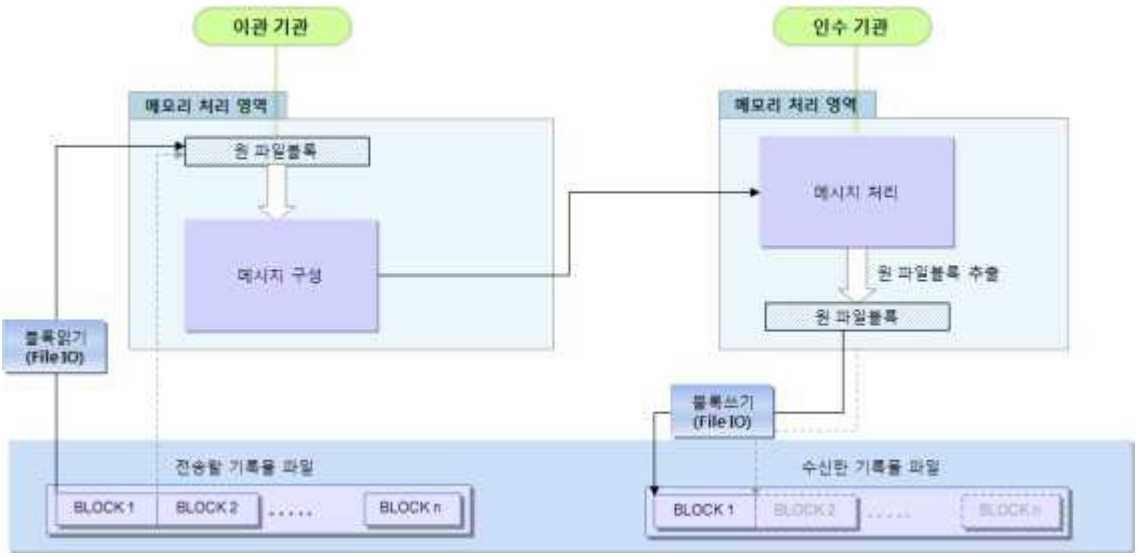

그림 2 - 블록단위 파일전송

4.2.2 데이터 압축 처리

데이터 압축은 데이터를 더 작은 크기로 변환시키는 '인코딩 과정'과 저장된 데이터를 다시 불러와 원래 데이터 형태로 복원시키는 '디코딩 과정'으로 이루어져야 하며, 전송하기 위한 세분화된 파일블록의 전송정보를 실시간으로 압축할 수 있어야 한다.

전송되는 전자기록물파일의 압축처리 여부는 전송목록파일에 명기된 압축여부에 따라 선택적으로 적용되어야 한다.

전자기록물 온라인 전송에 적용되는 압축 알고리즘은 전자기록물의 내용을 바꾸지 않고 원래 내용 그대로 디코딩할 수 있는 무손실 압축 알고리즘을 적용하며, RFC1951 및 일반 상용소프트웨어, 오픈소스에서 일반적으로 제공되는 Deflate 알고리즘을 이용하여야 한다.

4.2.3 암호화 처리

전자기록물의 암호화 처리는 SSL/TLS(RFC2246, RFC4345) 네트워크 보안을 이용하여 송・수신모듈 간 기밀성을 보장하여야 한다.

전송소프트웨어는 전자기록물의 암호화 처리를 위해 SSL/TLS와 연계하여 전송한다. SSL/TLS는 클라이언트와 서버 간 handshake 단계를 거친 후에 Cipher Data Transaction을 수행하는데, 전송데이터 암호화 시 사용되는 알고리즘은 SEED 대칭키 블록암호 알고리즘이 지원되어야 하고, SEED 대칭키의 키 정보는 Handshake 단계에서 규격에 의해 생성되어야 한다.

SSL/TLS는 Class2, Class3이 지원되어야 하고, SSL/TLS의 handshake 단계에서는 서버 인증서 검증을 수행하여 신뢰성을 확보하여야 한다. 그리고 전송되는 전자기록물의 암호화 처리여부는 전송목록파일에 명기된 암호화 여부에 따라 선택적으로 적용할 수 있어야 한다.

4.2.4 재전송/이어보내기

재전송은 장애요인 복구 시 전송 완료된 파일 또는 파일블록을 다시 전송하는 기능이며, 전송된 파일은 전송 완료된 최종 파일만 관리되어야 한다.
이어보내기는 장애요인 복구 시 전송 완료된 이후의 파일 또는 파일블록부터 전송하는 기능이며, 송・수신측은 전송할 파일에 대해 매번 최신의 수신상태를 검사하여야 한다. (**그림 3** 참조)

재전송 및 이어보내기는 송・수신모듈 모두 적용되어야 한다.

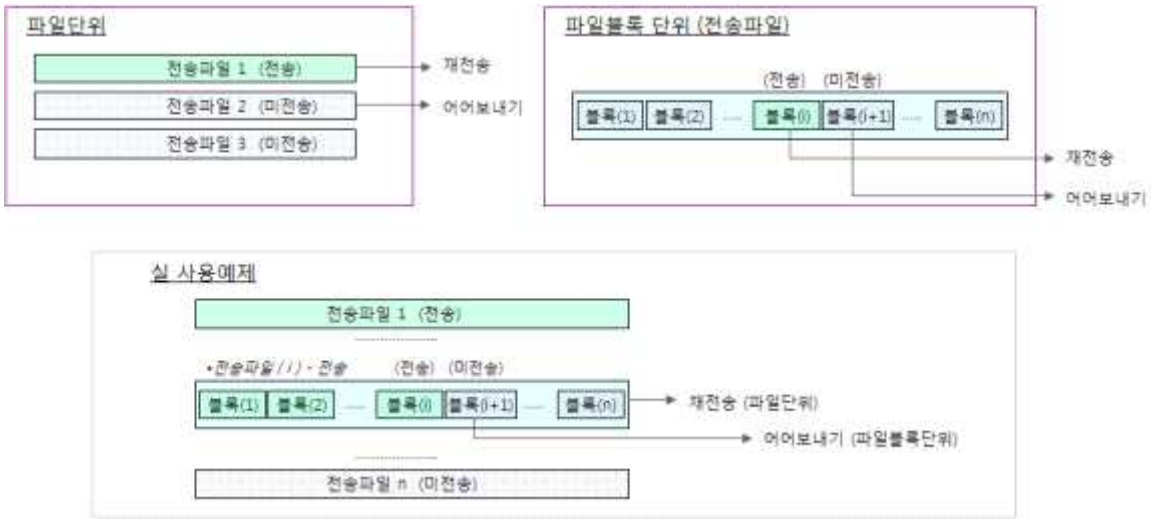

그림 3 - 재전송 및 이어보내기

4.2.5 메시지 무결성 정보 생성

전송 중인 메시지에 대한 위·변조 여부를 확인할 수 있도록 무결성 정보를 포함하여야 하고, 이때 사용되는 무결성 정보는 SHA-1(참고문헌 [6]) 혹은 SHA-2(참고문헌 [7]) 해쉬 알고리즘을 이용하여 생성한다. 메시지 무결성 검증을 위해 송신모듈은 해쉬 알고리즘을 이용하여 body 부분의 무결성 정보를 생성하고, 수신모듈은 동일 해쉬 알고리즘을 이용하여 무결성 정보를 검증한다. (**그림 4** 참조)

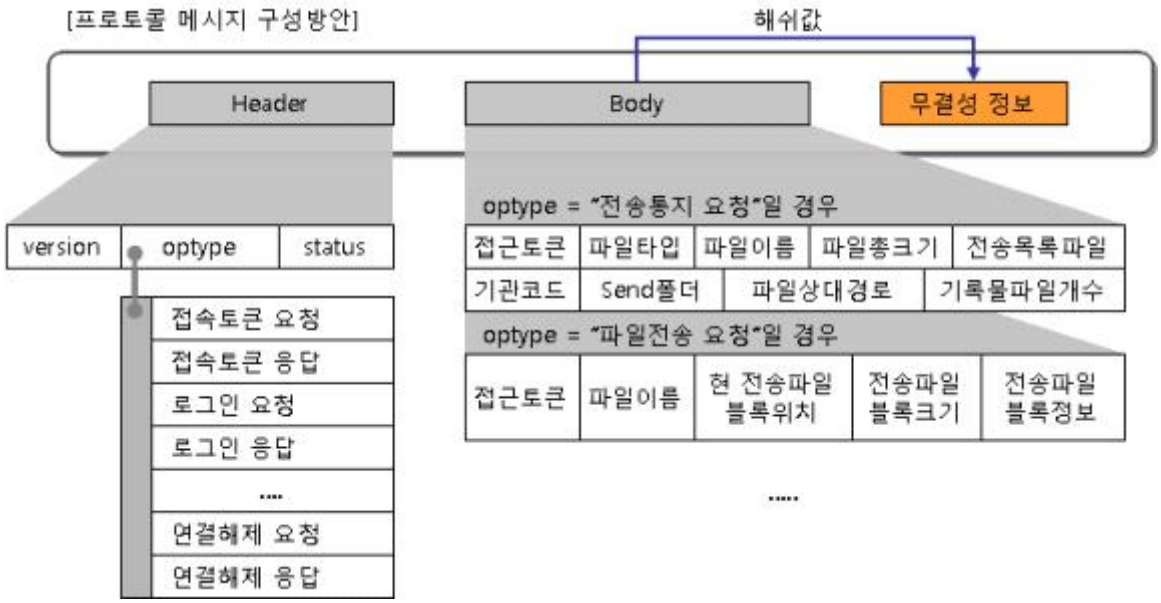

그림 4 - 전송정보 무결성 생성

4.2.6 파일 일치성 보장

기록물 파일 전송 시, 송신한 기록물이 수신한 기록물과 일치함이 반드시 보장되어야 한다. 파일 일치성을 보장하기 위해서는 전송목록파일에 기입된 모든 파일리스트의 파일명, 확장자 및 파일크기가 수신한 파일과 일치하도록 보장되어야 한다.

4.2.7 수신이력 시각정보 생성

수신이력에 대한 증적정보 확보를 위하여 수신완료 시 수신이력에 대한 시점확인 토큰을 생성하여야 하며 이때 사용되는 수신이력은 전송목록파일을 사용하고 시점확인 토큰은 RFC3161 시점확인 토큰 표준을 준용한다. (참고문헌 [3])

수신이력 시각정보 생성은 수신한 파일에 대해 파일 일치성이 보장된 경우에 한하여 수행되어야 한다. **그림 5**는 시점확인 토큰 생성을 위한 절차를 나타내며, 세부절차에 대한 설명은 '6.2.5 [P4] 시점확인토큰 생성 세부 흐름도'의 **그림 22**를 참조한다.

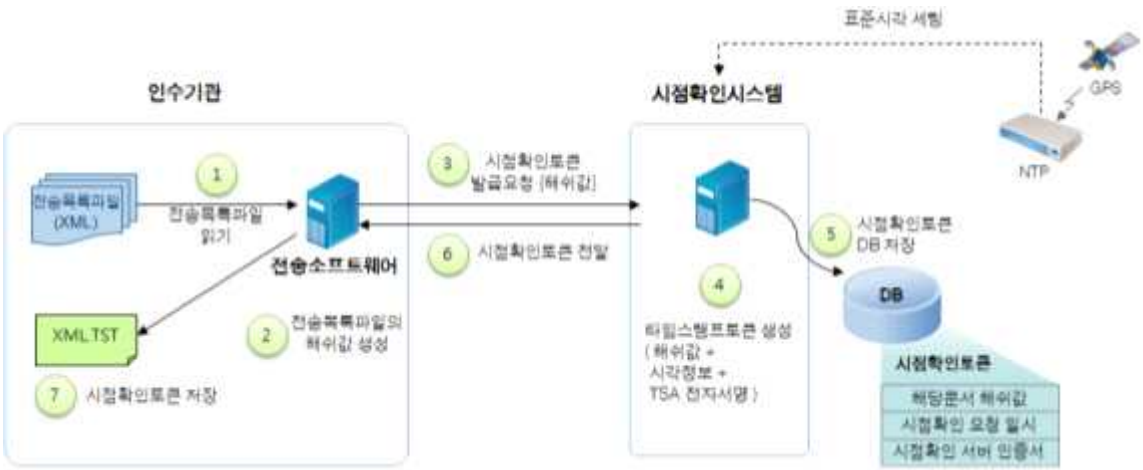

그림 5 - 수신이력 시각정보 생성

4.2.8 다중세션 전송

수신모듈은 하나 또는 다수의 송신모듈을 통하여 전자기록물파일을 병렬적으로 수신할 수 있어야 하며 이때 각 송신모듈은 전송목록파일, 전자기록물파일, 전송완료파일 순서로 전송하여야 한다.

또한 송신모듈은 효율적 전송을 위해 전송할 파일 단위로 세션을 생성하여 병렬적으로 전송할 수 있어야 하며 송신모듈의 다중세션 최대 개수는 수신모듈의 가용 자원에 따라 제약되어야 한다.

각 세션은 인증을 거친 후 생성되고, 파일전송이 완료된 후에는 반드시 세션을 종료하여야 한다.

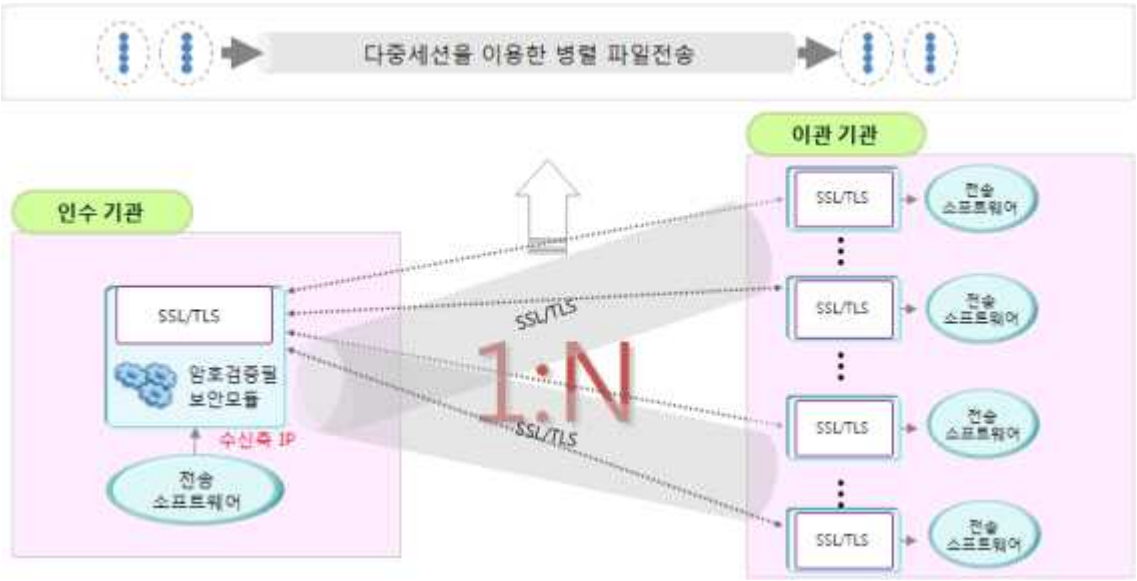

그림 6 - 다중세션 개념도

4.2.9 사용자 인증

전자기록물 송·수신 기능 수행 시, 반드시 송·수신 모듈간의 인증절차를 수행하여야 한다. 인증방식은 '인증서 기반' 방식과 'ID/패스워드'방식 둘 중 하나를 반드시 사용하여야 하며, 인증서 기반인 경우 PKCS#7의 SignedData를 이용하여야 한다. (참고문헌 [11])

시스템 운영의 편의성을 위해, 송신모듈(이관기관)은 오프라인을 통해 수신모듈(인수기관)에 인증정보를 등록하고, 송신모듈이 수신모듈에 최초 로그인 시 인수기관의 인증정보를 1회 전달하는 방식을 이용한다.

인증정보는 기관ID, 패스워드, 그리고 인증서 DN은 필수항목이고, 관리방안은 구현에 국한된 내용으로 이 규격에서 제약하지 않는다.

그림 7 - 사용자 인증절차도

5 업무시스템과의 연계 인터페이스

이 절에서는 업무시스템과 전송소프트웨어 간의 연계를 위한 규격을 정의한다. 업무시스템과 전송소프트웨어 간의 연계는 '5.1 디렉토리 구성', '5.2 전송목록파일', '5.3 업무시스템과 송·수신모듈 간 인터페이스' 규격으로 구분하여 상호 연계된다.

5.1 디렉토리 구성

송신 측 업무시스템은 '기관코드' 디렉토리 내에 send 디렉토리를 생성하여 전송할 전자기록물파일을 저장하고, 전송목록파일은 sendlist 디렉토리에 저장한다.

수신 측 전송소프트웨어는 먼저 수신한 전송목록파일을 recvlist 디렉토리 내에 저장한 후, 이어서 수신한 전자기록물파일을 '기관코드' 디렉토리 내의 receive 디렉토리에 저장한다. 이때 송신측의 send 디렉토리와 수신측의 receive 디렉토리는 하위 디렉토리 및 파일정보가 동일하여야 한다.

송신 측 전송소프트웨어는 전송이 완료된 전송목록파일 및 전자기록물파일을 sendcomplete 디렉토리에 이동하여야 하고, 수신 측 전송소프트웨어는 업무시스템의 접수처리가 완료된 전송목록파일 및 전자기록물파일을

recvcomplete 디렉토리로 이동하여야 한다. 업무시스템의 접수처리 완료여부는 '전송목록파일.complete' 파일의 존재 여부로 판단한다.

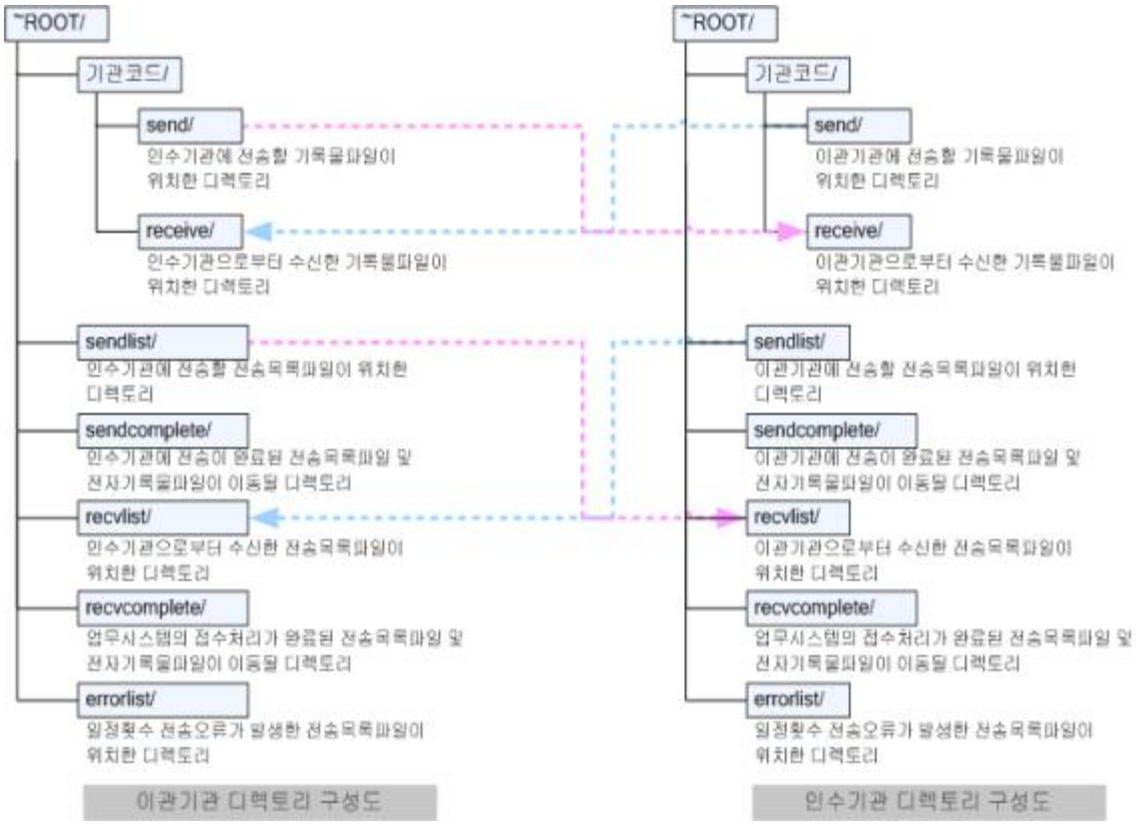

그림 8 - 송·수신측 디렉토리 구조

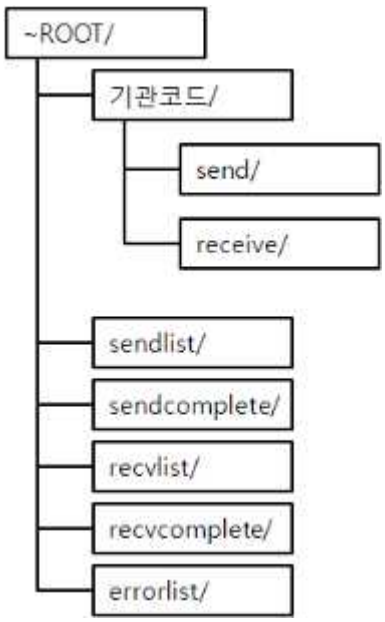

그림 9 - 디렉토리구성

표 2 - 디렉토리 구성

디렉토리 구성	반복수	설명
~ROOT/	1..1	• 업무시스템과 전송소프트웨어 간에 약속된 Base 디렉토리 경로 • ROOT 디렉토리는 유일해야 함 • 본 경로명은 예제로, 구축 환경에 따라 변경가능
기관코드/	1..*	• 기관을 구분하기 위한 디렉토리명 • 본 디렉토리명은 예제로, 해당 기관코드값을 가지는 디렉토리명이 사용됨 • send와 receive 하위 디렉토리를 반드시 가져야 함 • 기관별 기관코드값을 가지는 독립적인 디렉토리로, ROOT 디렉토리 하위에 기관개수에 비례하여 다수개 생성 예를 들어, ~ROOT 하위에 131001, 131002, 131003 등의 다수기관 디렉토리 생성
send/	1..1	• 수신모듈에 전송될 전자기록물파일이 위치한 디렉토리명 • 전자기록물파일 또는 하위 디렉토리 구조를 가질 수 있음 • send 디렉토리는 기관코드 하위에 생성되는 디렉토리명으로 기관코드 별로 유일해야 함 • 디렉토리명은 규정된 이름으로 변경 불가
receive/	1..1	• 송신모듈로부터 수신한 전자기록물파일이 위치한 디렉토리명 • 전자기록물파일 또는 하위 디렉토리 구조를 가질 수 있음 • receive 디렉토리는 기관코드 하위에 생성되는 디렉토리명으로 기관코드 별로 유일해야 함 • 디렉토리명은 규정된 이름으로 변경 불가
sendlist/	1..1	• 수신모듈에 전송할 전송목록파일이 위치한 디렉토리명 • 전송목록파일 또는 하위 디렉토리 구조를 가질 수 있음 • 전송소프트웨어는 sendlist를 포함한 하위디렉토리 내의 모든 전송목록파일에 대해 전자기록물 전송을 수행할 수 있어야 함 • sendlist 디렉토리는 ROOT 하위에 유일해야 함 • 디렉토리명은 규정된 이름으로 변경 불가
sendcomplete/	1..1	• 전송이 완료된 전송목록파일 및 전자기록물파일이 위치한 디렉토리명 • sendcomplete 디렉토리는 ROOT 하위에 유일해야 함 • 전송이 완료된 전송목록파일(.xml) 및 관련파일들(.end, .complete) 그리고 해당 전자기록물파일을 모두 이동해야 함 • 디렉토리명은 규정된 이름으로 변경 불가 • sendcomplete 하위 디렉토리 구성방안은 각 기관의 파일정책에 따라 기관의 특성을 반영하여 구성할 수 있다. 단, 전송목록파일과 전자기록물파일이 위치할 디렉토리는 반드시 구분되어야 함

	recvlist/	1..1	• 송신모듈로부터 수신한 전송목록파일이 위치한 디렉토리명 • 전송목록파일 또는 하위 디렉토리 구조를 가질 수 있음 • 전송목록파일 수신 완료시, sendlist의 하위 디렉토리 구조와 동일하게 구성할 수 있어야 함 • recvlist 디렉토리는 ROOT 하위에 유일해야 함 • 디렉토리명은 규정된 이름으로 변경 불가
	recvcomplete/	1..1	• 업무시스템의 접수처리가 완료된 전송목록파일 및 전자기록물파일이 위치한 디렉토리명 • recvcomplete 디렉토리는 ROOT 하위에 유일해야 함 • 접수처리가 완료된 전송목록파일(.xml) 및 관련파일들(.end, .complete, .tst) 그리고 해당 전자기록물파일을 모두 이동해야 함 • 디렉토리명은 규정된 이름으로 변경 불가 • recvcomplete 하위 디렉토리 구성방안은 각 기관의 파일정책에 따라 기관의 특성을 반영하여 구성할 수 있다. 단, 전송목록파일과 전자기록물파일이 위치할 디렉토리는 반드시 구분되어야 함
	errorlist/	1..1	• 일정횟수 오류가 발생한 전송목록파일이 위치한 디렉토리명 • errorlist 디렉토리는 ROOT 하위에 유일해야 함 • 전자기록물파일 전송시 일정횟수 오류가 발생한 전송목록파일(.xml) 및 관련파일들을 자동으로 이동해야 함 • 관련파일은 '.end', '.transferring', '.error' 등이 있을 수 있음 • 디렉토리명은 규정된 이름으로 변경 불가

비고 반복수는 해당 디렉토리의 {최소개수..최대개수}이며, *는 무한대를 나타낸다.

표 3 - 전자기록물 관리

처리 내역		송신모듈	수신모듈
성공 시 (.complete 존재)	전자기록물파일	'sendcomplete' 디렉토리로 이동	'recvcomplete' 디렉토리로 이동
	전송목록파일	'sendcomplete' 디렉토리로 이동	'recvcomplete' 디렉토리로 이동
실패 시 (.complete 존재하지 않음)	전자기록물파일	이동 없음	이동 없음
	전송목록파일	'errorlist' 디렉토리로 이동 전송목록파일.error도 이동	이동 없음

5.2 전송목록파일

5.2.1 전송목록파일 구조

전송목록파일은 전송할 전자기록물파일 정보를 기술한 파일로서, XML 형식으로 표현하여야 한다.

전송목록파일은 송신측 업무시스템에서 생성한 정보로 '5.1 디렉토리 구성'에서 정의한 디렉토리(sendlist)에 위치하여야 한다. 전송소프트웨어는 지정된 디렉토리 내의 하위 디렉토리를 포함한 모든 전송목록파일을 처리할 수 있어야 한다.

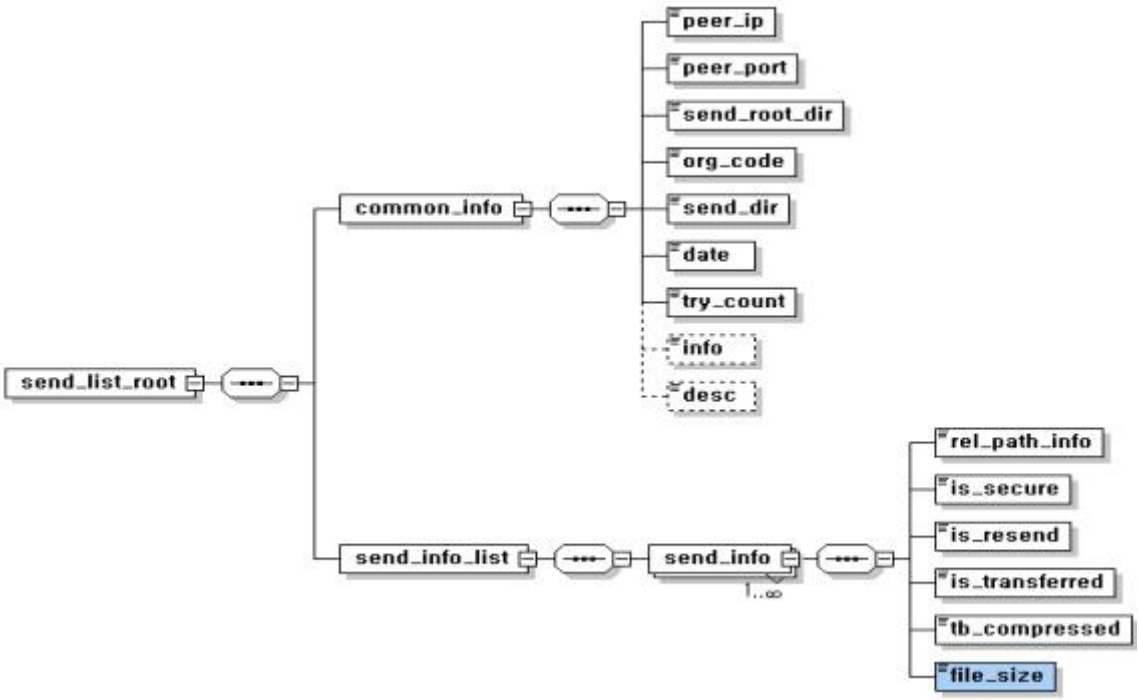

그림 10 - 전송목록파일(XML) 구조

표 4 - 전송목록파일 구조 설명

구성요소	반복수	타입	설명
send_list_root	1..1	-	• 전송목록파일 정보
common_info	1..1	-	• 공통적으로 적용될 정보
peer_ip	1..1	string	• 수신모듈 접속IP주소 • send_info_list에 나열된 파일에 공통적용 • 생성주체: 업무시스템

구성요소	반복수	타입	설명
peer_port	1..1	string	• 수신모듈 접속포트 • send_info_list에 나열된 파일에 공통적용 • 생성주체: 업무시스템
send_root_dir	1..1	string	• 전송할 전자기록물 저장 루트디렉토리 경로 • 절대경로를 기술하고, '/'로 종료 • 생성주체: 업무시스템
org_code	1..1	string	• 이관기관의 기관코드 • 생성주체: 업무시스템
send_dir	1..1	string	• 디렉토리구조에서 명기한 'send' 디렉토리명 • 생성주체: 업무시스템
date	1..1	string	• 전송목록파일 생성시간 (yyyyMMddHHmmss) • 생성주체: 업무시스템
try_count	1..1	string	• 해당 전송목록파일 내 전자기록물파일 전송 시도횟수 • 생성주체: 전송소프트웨어
info	0..1	string	• 전송할 전자기록물파일 개수 또는 기타 정보 기술 • 생성주체: 업무시스템
desc	0..1	string	• 전송 전자기록물에 대한 개략설명 • 생성주체: 업무시스템
send_info_list	1..1	-	• 전송 전자기록물파일 정보
send_info	1..*	-	• 전송대상 전자기록물파일 정보
rel_path_info	1..1	string	• 전송대상 전자기록물파일명 • 전자기록물파일이 위치한 파일의 send_dir 이후 상대경로로, 0개 이상의 디렉토리명과 1개의 파일명으로 구성되고 경로 구분자는 '/'를 사용한다. • 생성주체: 업무시스템
is_secure	1..1	string	• 암호화 전송여부 (1:암호화, 0:비암호화) • 암호화 전송일 경우에는 SSL/TLS을 통해 전자기록물파일을 전송 • 생성주체: 업무시스템
is_resend	1..1	string	• 재전송 여부 (0:초기전송, 1:재전송) • 재전송 여부를 매뉴얼 방식으로 '1'로 설정 시, 'is_transferred'도 매뉴얼 방식으로 '0'으로 설정하여야 함 • 생성주체: 업무시스템
is_transferred	1..1	string	• 전송완료여부 (0:미전송, 1:전송완료) • 해당 파일에 대해 전송 완료 여부 • 업무시스템은 해당 엘리먼트를 생성하고, '0'으로 설정해야 함 • 전송소프트웨어는 해당 기록물파일을 성공적으로 전송완료 시 '1'

구성요소	반복수	타입	설명
			로 설정해야 함 ● 생성주체: 전송소프트웨어
tb_compressed	0..1	string	● 전송대상파일 압축여부 (0:비압축, 1:압축) ● 생성주체: 업무시스템
file_size	1..1	string	● 전송대상 파일크기 ● 업무시스템은 해당 엘리먼트를 생성하고, 공백(empty)으로 설정해야 함 ● 전송소프트웨어는 전송목록파일을 전송하기 전에 해당 기록물파일의 크기를 설정해야 함 ● 생성주체: 전송소프트웨어

- 반복수 : 해당 엘리먼트의 {최소개수..최대개수}, *는 무한대를 나타낸다.
- 'try_count'는 해당 전송목록파일의 전자기록물파일 전송 시도 횟수를 나타내는 값으로, 초기 '1'이 설정되고, 1회 전송 시도 시 1을 증가시켜야 한다. 'try_count'의 증가는 전송목록파일 단위로, 전송목록파일 내 다수의 전자기록물 파일에 오류가 발생하더라도 이는 1회로 산정한다.
- 전송소프트웨어는 해당 전송목록파일 관련 모든 전자기록물파일이 전송완료되거나 업무시스템에서 접수처리가 완료되면, 관련 파일들을 'sendlist'에서 'sendcomplete' 또는 'recvlist'에서 'recvcomplete' 디렉토리로 이동시켜야 한다.
- 전송소프트웨어는 지정한 일정 횟수 동안 전자기록물파일 전송에 실패하면 해당 전송목록파일 관련 모든 파일을 'sendlist'에서 'errorlist' 디렉토리로 이동시켜야 한다.
- 전자기록물파일 경로는 send_root_dir+org_code + '/' + send_dir + '/' + rel_path_info 로 구성하여야 한다.
- is_resend가 '1'로 설정된 경우, 송신모듈은 해당파일(rel_path_info)을 재전송해야 하고, 재전송 파일블록은 '0'(처음블록)부터 진행한다. 즉, is_resend가 '1'인 경우 송신모듈은 해당 파일을 첫 번째 파일블록부터 전송하고, 수신모듈은 이를 처리할 수 있어야 한다.
- 송신모듈은 해당 전자기록물파일 전송이 완료되면 is_transferred를 '1'로 설정하여야 한다.
- 송신모듈은 업무시스템에서 생성한 전송목록파일에 대해, 파일크기(file_size)를 설정한 후 수신모듈에 전송하여야 한다.

5.2.2 전송목록파일 관리방안

전송목록파일은 업무시스템이 최초로 생성한다. 전송목록파일의 파일명은 '기관코드값'을 반드시 포함해야 하고, 동일한 이관기관에서 생성한 모든 전송목록파일명은 유일한 이름을 가져야 한다. 전송목록파일명의 명명규칙은 다음과 같다.

전송목록파일명 : = '기관코드' + '파일명' + '[.확장자]'
- 기관코드 : 이관기관의 기관코드 값 (문자열로 표기)
- 파일명 : 이관기관에서 자유로이 부여 가능
- 확장자 : 생략가능
- 제약사항 : 확장자를 포함한 파일명은 기관 내에서 유일

전송소프트웨어는 처리단계 별로 동일한 전송목록파일명에 확장자가 다른 파일로 생성하여야 한다. 생성된 파일들은 sendlist나 recvlist 디렉토리에 위치하도록 한다.

(a) 송신 측

표 5 - 송신 측 전송목록파일 관리방안

확장자 구분	파일크기	생성자	생성시기
.xml	가변	업무시스템	전송목록파일 생성 시작
.end	0 바이트	업무시스템	전송목록파일 생성 완료
.transferring	0 바이트	전송소프트웨어	전송목록파일 내 전자기록물파일 전송진행
.complete	0 바이트	전송소프트웨어	전송목록파일 내 전자기록물파일 전송완료
.error	가변	전송소프트웨어	오류 발생 시점

- 파일위치 경로: 'sendlist' 디렉토리 내 전송목록파일(.xml)과 동일 경로
- '.complete' 파일은 전송목록파일에 대해 파일 일치성이 보장될 때 생성되고, '.complete' 파일이 생성되면 '.transferring' 파일은 삭제된다.
- 전송소프트웨어는 전송목록파일의 확장자가 '.end'가 존재하고,

'.complete'이 존재하지 않은 파일에 한해 전송을 수행한다.

- '.error' 파일은 전송목록파일에 대해 처리 도중 오류 발생 시, 해당파일은 실패로 처리하고 이후의 전자기록물 전송을 계속 진행한다. 전송목록파일 자체에 대한 오류 시는 다음 전송목록파일 처리로 이동하고, 전송파일목록 내 임의의 전자기록물파일 처리 시 오류가 발생하면 다음 처리할 전자기록물파일 전송을 계속 수행한다.
- 전송이 완료된 전송목록파일(.xml) 및 관련파일들(.end, .complete)은 'sendlist'에서 'sendcomplete' 디렉토리로 이동시킨다.
- 전송소프트웨어는 전송목록파일 내 'try_count'가 일정 오류횟수에 도달하면, 해당 전송목록파일(.xml) 및 오류파일(.error)을 포함한 관련 모든 파일들을 'sendlist'에서 'errorlist' 디렉토리로 이동시켜서 이후 전송대상에서 제외한다.
- 오류파일 포맷은 '6.4.2 오류내역을 위한 로그포맷'에서 정의한다.

(b) 수신 측

표 6 - 수신 측 전송목록파일 관리방안

확장자 구분	파일크기	생성자	생성시기
.xml	가변	전송소프트웨어	전송목록파일 수신완료
.end	0 바이트	전송소프트웨어	모든 전자기록물파일 수신 후, 파일 일치성 검사완료
.tst	가변	전송소프트웨어	기록물파일 수신완료 통보 및 로그아웃 처리 완료
.complete	0	업무시스템	전자기록물 접수처리 완료
.error	가변	전송소프트웨어	오류 발생 시점

- 파일위치 경로는 recvlist 디렉토리 내 전송목록파일 동일 경로에 위치하여야 한다.
- '.end'파일은 전송소프트웨어가 전자기록물파일을 성공적으로 수신완료했음을 나타내는 정보로, 파일 일치성 검사 완료 후에 생성되어야 한다.
- '.tst'파일은 해당 전송목록파일에 대해 파일 일치성 검사 성공 시에만 생성되는 파일이어야 한다.

- '.complete'파일은 수신한 전자기록물파일을 업무시스템이 접수처리를 완료했음을 나타내는 정보로, 업무시스템이 생성한다.
- 업무시스템은 해당 전송목록파일에 대해 확장자가 '.complete'파일이 존재하지 않고, '.end' 및 '.tst' 파일이 존재한 경우 한해 접수업무를 수행하여야 한다.
- 업무시스템의 접수처리가 완료된 전송목록파일(.xml) 및 관련파일들(.end, .complete, .tst)은 'recvlist'에서 'recvcomlete' 디렉토리로 이동시킨다. 접수처리가 완료된 시점은 '.complete'의 존재로 판단하여야 한다.
- 전송소프트웨어는 해당 전송목록파일(.xml) 처리 중 일정횟수 재전송 실패, 송신모듈 오류메시지 전달, 파일 일치성 검사 오류 등과 같은 오류가 인지된 경우 ".error" 파일에 해당내역을 기입한다. 본 규격에서는 수신모듈의 .error 파일 관리는 제약하지 않는다.

5.2.3 구 전송목록파일 수용방안

기 비표준 대용량 솔루션을 사용 중인 업무시스템과의 연계를 위해 전송소프트웨어의 송신모듈은 다음의 내역을 추가로 처리할 수 있어야 한다.

업무시스템은 기 대용량 솔루션에서 정의한 전송목록파일의 규격을 준용해야 하고, 신규 전송소프트웨어는 기존의 전송목록파일을 기반으로 '5.2.1 전송목록파일 구조' 및 '5.2.2 전송목록파일 관리방안'에서 기술된 항목을 만족해야 한다.

(a) 전송목록파일 재구성

기 비표준 대용량 솔루션을 통해 업무시스템에서 생성한 전송목록파일을 다음의 규칙에 의해 신규 전송목록파일로 자체 생성할 수 있어야 한다.

구성요소 (기존)	설명
send_list_root	• 전송목록파일 정보
common_info	• 공통적으로 적용될 정보
peer_ip	• 생성주체: 업무시스템
peer_port	• 생성주체: 업무시스템

구성요소 (신규)	설명
send_list_root	• 전송목록파일 정보
common_info	• 공통적으로 적용될 정보
peer_ip	• 설정정보 유지 • 생성주체: 업무시스템
peer_port	• 설정정보 유지

send_root_dir	• 생성주체: 업무시스템
rm_code	• 생성주체: 업무시스템
send_dir	• 생성주체: 업무시스템
date	• 생성주체: 업무시스템
send_info_list	• 이관 전자기록물파일 정보
send_info	• 이관대상 전자기록물파일 정보
rel_path_info	• 생성주체: 업무시스템
is_secure	• 생성주체: 업무시스템
is_resend	• 생성주체: 업무시스템
is_registered	• 생성주체: 전송소프트웨어

	• 생성주체: 업무시스템
send_root_dir	• 설정정보 유지 • 생성주체: 업무시스템
org_code	• rm_code 설정정보 사용 • 생성주체: 전송소프트웨어
send_dir	• 설정정보 유지 • 생성주체: 업무시스템
date	• 설정정보 유지 • 생성주체: 업무시스템
try_count	• 생성주체: 전송소프트웨어
info	• 생성주체: 전송소프트웨어
desc	• 생성주체: 전송소프트웨어
send_info_list	• 이관 전자기록물파일 정보
send_info	• 이관대상 전자기록물파일 정보
rel_path_info	• 설정정보 유지 또는 변경 • 생성주체: 공통
is_secure	• 설정정보 유지 • 생성주체: 업무시스템
is_resend	• 설정정보 유지 또는 변경 • 생성주체: 업무시스템
is_transferred	• is_registered 설정정보 사용 • 생성주체: 전송소프트웨어
tb_compressed	• 생성주체: 전송소프트웨어
file_size	• 생성주체: 전송소프트웨어

- “org_code”는 기존 전송목록파일의 “rm_code"의 설정정보를 사용한다.
- 기존 전송목록파일의 “rel_path_info"가 디렉토리명으로만 구성되어 있는 경우에는 전송소프트웨어의 송신모듈은 해당 디렉토리 내의 모든 파일명에 대해 ”send_info"를 생성한다. 이때 “send_info" 하위의 나머지 설정정보는 그대로 유지한다.
- 전송소프트웨어는 전자기록물을 온라인으로 전송 시 새로 생성된 전송목록파일을 기반으로 전송을 수행해야 한다.

(b) 전송목록파일 관리

업무시스템이 생성한 전송목록파일(.xml, .end)이 ‘5.2.2 전송목록파일 관리방안’에서 기술한 명명규칙을 준용하지 않은 경우, 전송소프트웨어 송신모듈은

명명규칙에 준해 전송목록파일을 생성한 후 기존의 전송목록파일은 삭제한다.

5.3 업무시스템과 송·수신모듈 간 인터페이스

전자기록물 송신을 위한 업무시스템과 송신모듈 간 '전자기록물 전송요청' 인터페이스는 송신 측의 아래 표준 인터페이스를 이용하여 요청하여야 한다.

수신 측의 경우 전송목록파일에 대한 시점확인토큰 생성 후, 업무시스템에서 제공한 '접수처리 기능'을 구동할 수 있어야 한다.

표준 인터페이스 정의는 표 7을 참고하여 구현할 수 있다.

표 7 - 표준 인터페이스 정의

기능명	비고
reqARCSend	· 업무시스템이 전자기록물 전송과 접수를 수행하기 위한 전송소프트웨어 간의 연계 표준인터페이스를 나타낸다. · 업무시스템은 reqARCSend 기능을 구현하여 업무시스템에 적용한다. · reqARCSend의 세부기능은 전송소프트웨어를 구현하는 제품에 의존하므로, 제품에서 제공한 라이브러리를 import한다. · 업무시스템이 reqARCSend를 호출하면 전송소프트웨어에서 제공한 라이브러리에 의해 전자기록물 전송요청이 이루어진다.

함수정의 원형	reqARCSend		
기능개요	전송소프트웨어에 전자기록물 전송요청		
구 분	명칭	타입	설명
파라미터	-	-	-
결 과	retCodeString	String	전송요청에 대한 처리 응답코드값
오 류	에러코드 전달		
설 명	· sendlist 디렉토리 내 전송목록파일에 대해 전송요청을 수행하여야 한다. · sendlist의 지정된 디렉토리 경로는 전송소프트웨어에서 별도 관리하여야 한다. · 전자기록물 전송요청 인터페이스는 전송목록파일 검사 후 검사결과를 리턴(E01XX)하여야 하고, 전송 중 발생한 오류정보는 '6.4.2 오류내역을 위한 로그포맷'에 기술된 로그파일을 이용하여 전송 중 발생된 오류내역을 참조한다. · 해당 전송목록파일에 대한 전송상태는 '5.2.2 전송목록파일 관리방안'에서 기술한 전송목록파일의 확장자를 이용하여 판단하여야 한다.		

6 송·수신 프로토콜

이 절에서는 전자기록물을 전송하기 위한 프로토콜 동작 절차, 프로세스 동작 절차, 메시지 규격, 로그포맷에 대해 기술한다.

'6.1 프로토콜 동작 절차'에서는 송·수신모듈 간 메시지 전송을 위한 프로토콜 규격을 정의하고, '6.2 프로세스 동작 절차'에서는 프로토콜 규격을 포함한 송·수신 메시지 처리 절차를 정의한다. '6.3 메시지 규격'에서는 송·수신 메시지의 포맷을 정의하고, '6.4 로그포맷'에서는 오류 처리 및 이력 관리를 위한 로그 포맷을 정의한다.

6.1 프로토콜 동작 절차

6.1.1 소켓연결 절차

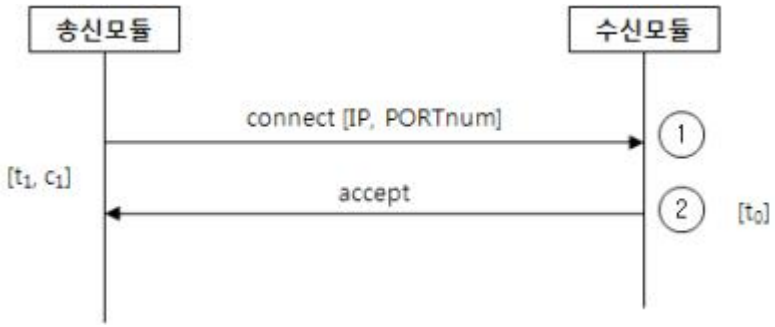

그림 11 - 소켓연결 절차

○ 정의

소켓연결 절차는 송신모듈이 수신모듈에 tcp socket으로 연결을 수행하는 절차이다.

○ 동작절차

① 송신모듈은 수신모듈로 tcp socket 연결을 요청한다. (socket interface)
② 수신모듈은 송신모듈로부터 수신한 tcp socket 연결을 수락한다. (socket interface)

[t0] 수신모듈은 송신모듈과 연결된 세션으로 t0 시간 이내에 송신모듈의 요청이 없으면 tcp socket 연결을 해제하고 통신오류를 리턴한다.
[t1] 송신모듈이 연결을 요청한 후, t1 시간 이내에 수신모듈로부터 응답을 받지 못하면, 연결을 재요청한다.
[c1] 송신모듈은 c1번 연결을 재요청해도 응답이 없을 경우, '통신오류'를 리턴한다.

6.1.2 로그인 절차

그림 12 - 로그인 절차

○ **정의**

로그인 절차는 송·수신 모듈 간 상호인증을 위한 절차이다. 로그인 절차를 수행하기 위해서는 먼저 '접근토큰'을 수신해야 하고, 로그인을 성공하면 접근토큰은 세션별 추가적인 로그인 과정 없이 세션을 생성할 수 있다.

○ **동작절차**

① 송신모듈은 접근토큰 요청메시지(OP0001)를 생성하여 수신모듈로 전달한다.
② 수신모듈은 접근토큰을 생성한 후 접근토큰 요청에 대한 ACK로 접근토큰 응답메시지(OP0002)로 전달한다.
③ 송신모듈은 로그인 요청메시지(OP0003)를 생성하여 수신모듈로 로그인을 요청한다.
④ 수신모듈은 송신모듈로부터 수신한 로그인 요청메시지에 대해 검증 및 등록여부를 확인한 후, 로그인 요청에 대한 ACK로 로그인 응답메시지(OP0004)를 반송한다.
성공 로그인 응답메시지를 수신하면 해당 세션을 통해 전자기록물파일 전송이 가능하다.

[t2] 송신모듈이 로그인을 요청한 후, t2 시간 이내에 수신모듈로부터 응답을 받지 못하면, 로그인을 재요청한다.
[c2] 송신모듈은 c2번 재요청해도 응답이 없을 경우, '통신오류'를 리턴한다.

6.1.3 파일전송 시작통지 절차

그림 13 - 파일전송 시작통지 절차

○ 정의

파일전송 시작통지 절차는 파일전송을 위한 송·수신모듈 간 상호 협의절차로, 전송할 파일정보 및 수신모듈이 이미 수신 완료한 파일정보를 상호 확인한다.

○ 동작절차

① 송신모듈은 파일전송 시작통지를 위해 전송통지 요청메시지(OP0011)를 생성하여 수신모듈로 전달한다. 전송통지 요청메시지는 전송할 파일정보를 포함한다.
② 수신모듈은 송신모듈로부터 수신한 전송통지 요청메시지에 대한 ACK로 전송통지 응답메시지(OP0012)를 반송한다.
전송통지 응답메시지는 수신모듈이 이미 수신완료한 파일정보를 포함하여야 한다. 이미 수신한 내역이 없는 경우에는 수신완료한 크기를 '0'으로 설정하여야 한다.

[t3] 송신모듈이 전송통지를 요청한 후, t3 시간 이내에 수신모듈로부터 응답을 받지 못하면, 전송통지를 재요청한다.
[c3] 송신모듈은 c3번 재요청해도 응답이 없을 경우, 통신오류를 리턴한다.

6.1.4 파일전송 절차

그림 14 - 파일전송 절차

○ **정의**

파일전송 절차는 전자기록물파일을 파일블록 단위로 전송하는 절차이다.
파일블록을 전송하기 위해서는 반드시 '파일전송 시작통지 절차'를 수행한 후 수행하여야 한다.

파일전송 절차는 파일(또는 파일블록) 재전송기능이 지원되어야 하고, '파일전송 시작통지 절차'의 응답메시지에 따라 이어보내기 기능이 지원되어야 한다.

하나의 전자기록물파일이 전송완료 되기 위해서는 파일전송이 완료될 때까지 파일블록 단위 '파일전송 절차'를 반복 수행하여야 한다.

○ **동작절차**

① 송신모듈은 전송할 파일블록에 대한 파일전송 요청메시지(OP0013)를 생성하여 수신모듈로 전달한다. 파일전송 요청메시지는 전송할 파일정보 및 파일블록정보를 포함한다.
전송할 파일블록의 위치는 최초 전송 시, '파일전송 시작통지 절차'의 응답메시지인 respNotiMessage.currentFileSize 값에 의해 결정되고, 파일블록이 전송 중일 때에는 '파일전송 요청_ACK'인 파일전송 응답메시지(OP0014)의 respFileTransferMessage.totalFileSize에 의해 결정된다. respNotiMessage.currentFileSize가 양의 정수값을 가지면 송신모듈은 이어보내기 기능을 수행하여야 한다.
② 수신모듈은 송신모듈로부터 수신한 파일전송 요청메시지에 대한 ACK로 파일전송 응답메시지(OP0014)를 반송한다.

파일전송 응답메시지는 수신모듈이 성공적으로 수신완료한 파일블록 정보를 포함해야 한다. 만일 수신한 파일블록정보에 대한 검증이 실패할 경우에는 해당 파일블록을 지정된 횟수(c5)만큼 재전송을 요청해야 한다.

[t4] 송신모듈이 파일전송을 요청한 후, t4 시간 이내에 수신모듈로부터 응답을 받지 못하면, 파일전송을 재요청한다.

[c4] 송신모듈은 c4번 재요청해도 응답이 없을 경우, 통신오류를 리턴한다.

[c5] 수신모듈은 수신한 파일블록이 유효하지 않으면, c5번 횟수만큼 해당블록에 대해 재전송을 요청하여야 한다. 만일 횟수 이내에 유효한 파일블록을 수신하지 못하면 오류를 리턴한다.

6.1.5 파일전송 완료통지 절차

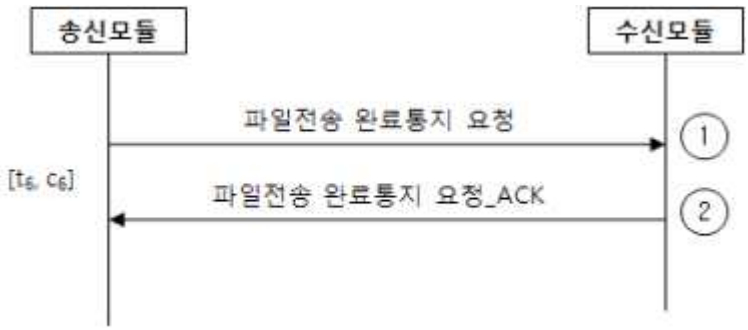

그림 15 - 파일전송 완료통지 절차

○ **정의**

파일전송 완료통지 절차는 전자기록물파일 전송이 완료되었음을 알리는 절차이다.

○ **동작절차**

① 송신모듈은 파일전송 완료통지를 위해, 전송통지 요청메시지(OP0011)를 생성하여 수신모듈로 전달한다. 전송통지 요청메시지는 전송이 완료된 전송목록파일 정보를 포함한다.

② 수신모듈은 송신모듈로부터 수신한 전송통지 요청메시지에 대한 ACK로 전송통지 응답메시지(OP0012)를 반송한다.

[t6] 송신모듈이 전송통지를 요청한 후, t6 시간 이내에 수신모듈로부터 응답을 받지 못하면, 전송통지를 재요청한다.
[c6] 송신모듈은 c6번 재요청해도 응답이 없을 경우, 통신오류를 리턴한다.

6.1.6 로그아웃 절차

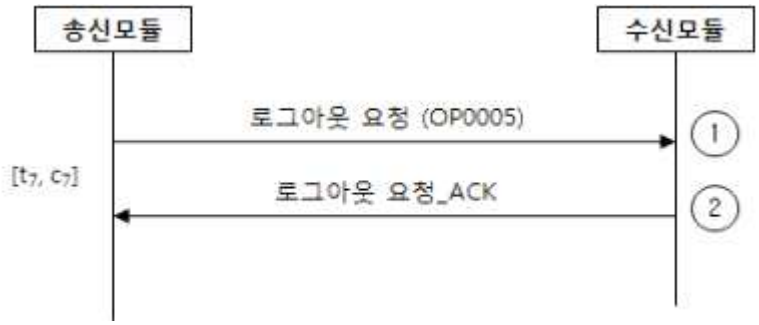

그림 16 - 로그아웃 절차

○ 정의

로그아웃 절차는 송・수신 모듈 간 로그아웃을 수행하기 위한 절차이다.

○ 동작절차

① 송신모듈은 로그아웃 요청메시지(OP0005)를 생성하여 수신모듈로 전달한다.
② 수신모듈은 로그아웃 요청에 대한 ACK로 로그아웃 응답메시지(OP0006)를 전달한다. 로그아웃 이후에는 상호 교환된 접근토큰은 더 이상 사용될 수 없다.

[t7] 송신모듈이 접근토큰을 요청한 후, t7 시간 이내에 수신모듈로부터 응답을 받지 못하면, 접근토큰을 재요청한다.
[c7] 송신모듈은 c7번 재요청해도 응답이 없을 경우, tcp socket 연결을 해제한다.

6.1.7 연결해제 절차

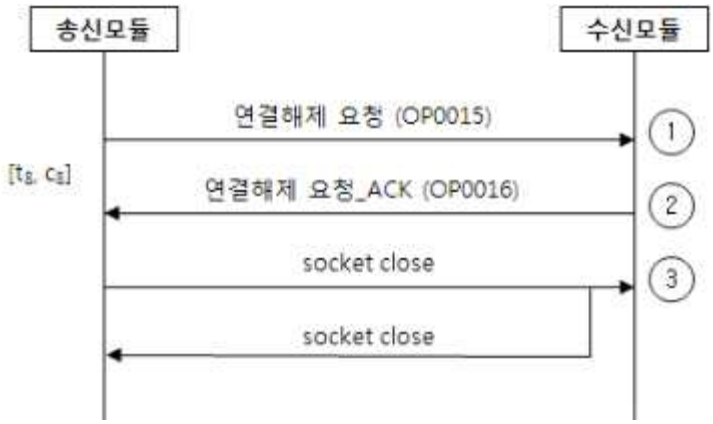

그림 17 - 연결해제 절차

○ 정의

연결해제 절차는 송·수신 모듈 간 tcp socket 연결을 해제하기 전에 자원 반납 등과 같은 일련의 작업을 종료한 후, tcp socket을 정상 종료하기 위한 절차이다.

○ 동작절차

① 송신모듈은 수신모듈과 연결을 해제하기 전에 자원반납 등과 같은 일련의 작업을 종료하기 위해, 연결해제 요청으로 연결해제 요청메시지(OP0015)를 수신모듈에 전달한다.
② 수신모듈은 해당 작업을 완료한 후, 연결해제 요청에 대한 ACK로 연결해제 응답메시지(OP0016)를 반송한다.
③ 송·수신 모듈은 tcp socket을 해제한다.

[t_8] 송신모듈이 연결해제를 요청한 후, t_8 시간 이내에 수신모듈로부터 응답을 받지 못하면, 연결해제를 재요청한다.
[c_8] 송신모듈은 c_8번 재요청해도 응답이 없을 경우, tcp socket 연결을 해제한다.

6.1.8 타이머 및 재요청 카운트

6.1.8.1 타이머

- t_0 : 120 초
- t_1 : 30 초
- t_2 : 30 초
- t_3 : 30 초
- t_4 : 30 초
- t_5 : 30 초
- t_6 : 30 초
- t_7 : 30 초
- t_8 : 30 초

6.1.8.2 재요청 카운터

- c_1 : 3 회
- c_2 : 3 회
- c_3 : 3 회
- c_4 : 3 회
- c_5 : 3 회
- c_6 : 3 회
- c_7 : 3 회
- c_8 : 3 회

6.2 프로세스 동작 절차

6.2.1 송・수신 모듈 간 전자기록물 전송절차

전송소프트웨어의 송신모듈은 업무시스템이 생성한 전자기록물파일 및 전송목록파일을 수신모듈에 전송하여야 한다. 전자기록물파일 및 전송목록파일은 '5 업무시스템과의 연계 인터페이스'를 준용하여야 한다.

그림 18은 전자기록물 전송절차를 그룹화 하여 기술한 것이다

전송소프트웨어의 전자기록물 전송은 반드시 'P1 전송목록파일 전송', 'P2 전자기록물파일 전송', 'P3 전송목록파일 전송완료 통보'의 절차로 진행되어야 하고, 각 절차 내에서 전송되는 정보는 별도의 세션을 통해 전송되어야 한

다. 즉, P1에서 생성된 세션이 P2에서 사용되지 않음을 나타낸다.

P1, P2, P3은 내부적으로 별도의 세부절차를 갖는다. P1은 '전송목록파일 전송'을 위한 프로토콜 절차를 수행하고, P2는 전송목록파일에 기술된 '전자기록물파일 전송'을 위한 프로토콜 절차를 수행한다. 그리고 P3은 해당 전송목록파일에 대한 '전송목록파일 전송완료 통보'를 위한 프로토콜 절차를 수행한다.

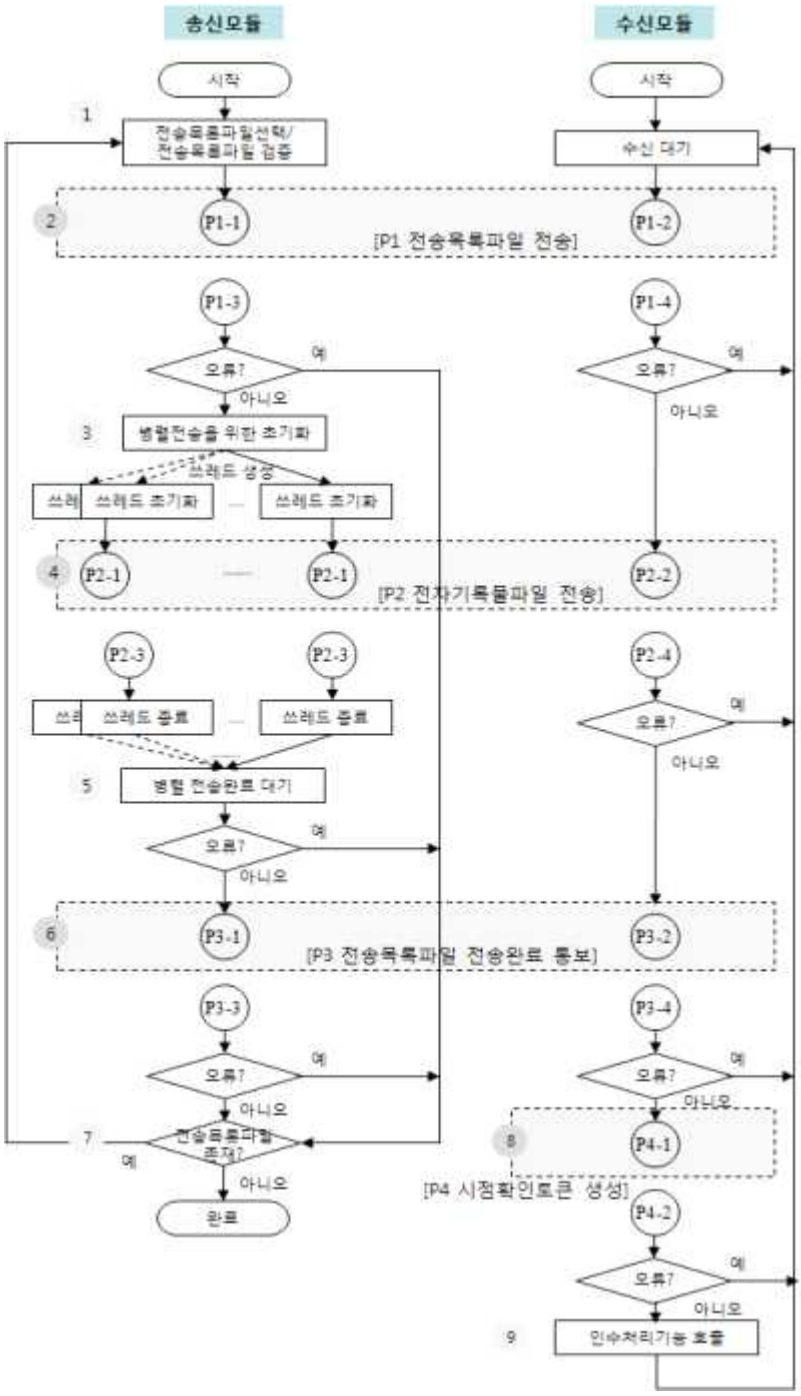

그림 18 - 전송소프트웨어 간 전자기록물 전송절차

① 전송목록파일 선택 및 전송목록파일 검증

- 전송할 전송목록파일을 선택한다. 전송할 전송목록파일은 전송목록파일의 확장자에 '.end'가 존재하고 '.complete'이 존재하지 않은 파일이 해당된다.
- 해당 전송목록파일에 대해 포맷, 전자기록물파일의 존재 여부 그리고 전송 시도 횟수(try_count)를 읽어와 검사한 후, 결과를 응용시스템에 리턴한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에 정의된 형식을 준용하여 로그파일로 기록한 후 절차 ⑦로 이동한다.
- 세부적인 절차는 '5.2 전송목록파일'의 규격을 참조한다.

② 전송목록파일 전송

- 송신모듈은 선택된 전송목록파일을 전송한다.
- 전송목록파일을 전송하기 위해서는 먼저 로그인 과정을 수행하고, 로그인 과정을 통해 공유된 '접근토큰'은 전자기록물 전송 시 정상적인 로그인 처리 여부를 나타내는 값으로 전자기록물 전송이 완료되는 시점까지 유지되어야 한다.
- 수신모듈은 수신한 전송목록파일을 'recvlist' 디렉토리에 저장한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에 정의된 형식을 준용하여 로그파일로 기록한 후, 송신모듈은 절차 ⑦로 이동한다.
- 세부적인 절차는 '6.2.2 [P1] 전송목록파일 전송 세부 흐름도'를 참조한다.

③ 병렬전송을 위한 초기화

- 전자기록물파일을 병렬로 전송하기 위해 쓰레드(또는 프로세스)를 설정된 개수만큼 생성한 후, 각 쓰레드(또는 프로세스)별로 전송할 전자기록물파일들을 할당한다.
- 이는 '다중세션 전송'을 위한 초기화 단계로, 각각의 쓰레드(또는 프로세스)는 ④의 단계를 동시에 독립적으로 수행한다.

④ 전자기록물파일 전송

- 전자기록물파일은 다중세션을 통해 전송하는 단계로, 송신모듈의 각각 쓰레드(또는 프로세스)는 할당된 전자기록물파일들을 독립적으로 전송한다.
- 수신모듈은 수신한 전송목록파일을 해당 디렉토리에 저장한다.

- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에 정의된 형식을 준용하여 로그파일로 기록한 후 나머지 업무를 계속 수행한다.
- 세부적인 절차는 '6.2.3 [P2] 전자기록물파일 전송 세부 흐름도'를 참조한다.

⑤ 병렬 전송완료 대기

- 송신모듈은 다중세션을 통해 전자기록물파일들이 전송 완료될 때까지 대기한다.
- 해당 전송목록파일에 대한 전송완료 통보는 모든 전자기록물파일들 전송이 완료된 시점에 이루어져야 하기 때문이다.

⑥ 해당 전송목록파일 전송완료 통보

- 송신모듈은 해당 전송목록파일에 대해 전송완료를 통보한다.
- 수신모듈은 수신한 해당 전송목록파일에 대한 파일 일치성 검사를 수행한 후, 일치성이 보장된 경우에 한해 지정된 디렉토리에 .end파일을 생성한다.
- 수신모듈은 파일 일치성 검사를 수행한 후, 전송목록파일 전송완료에 대한 응답을 리턴한다.
- 송신모듈은 성공응답을 수신하면 '.transferring' 파일을 삭제한 후 '.complete' 파일을 생성한다.
- 송신모듈은 전송이 성공적으로 완료된 전송목록파일(.xml) 및 관련 파일들(.end, .complete) 그리고 해당 전자기록물파일 들을 'sendcomplete' 디렉토리로 이동시켜야 한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에 정의된 형식을 준용하여 파일로 기록한 후, 송신모듈은 절차 ⑦로 이동한다.
- 세부적인 절차는 '6.2.4 [P3] 전송목록파일 전송완료 통보 세부 흐름도'를 참조한다.

⑦ 전송목록파일 존재 확인

- 송신모듈은 'sendlist' 내에 전송할 전송목록파일이 추가로 존재하는지 검사한 후, 존재하는 경우 ① ~ ⑥ 단계를 반복 수행한다.
- 전송할 전송목록파일은 전송목록파일의 확장자가 '.end'가 존재하고 '.complete'가 존재하지 않은 파일이 해당된다.

⑧ 시점확인 토큰 생성

- 수신모듈은 수신한 전송목록파일에 대한 시점확인 토큰을 생성한다.

- 세부적인 절차는 '6.2.5 [P4] 시점확인토큰 생성 세부 흐름도' 및 '5.2.2 전송목록파일 관리방안'을 참조한다.

⑨ 접수처리 기능 호출

- 송신모듈은 업무시스템에서 제공한 '접수처리 기능'을 구동한다.
- 세부적인 절차는 '5.3 업무시스템과 송·수신모듈 간 인터페이스'를 참조한다.

송신모듈은 해당 전자기록물의 전송 중 발생한 오류내역을 '5.2.2 전송목록파일 관리방안'에서 정의한 '.error' 파일에 기술하여야 한다.

수신모듈은 해당 전자기록물의 전송 중 발생한 오류내역 및 파일 일치성 검사 시 발생한 오류내역을 '5.2.2 전송목록파일 관리방안'에서 정의한 '.error' 파일에 기술하고 시점확인 토큰은 생성하지 않는다.

오류형식은 '6.4.2 오류내역을 위한 로그포맷'을 참조한다. 수신측 업무시스템은 '전송목록파일명.xml', '전송목록파일명.end', 그리고 '전송목록파일명.tst' 파일이 존재한 해당 전송목록파일에 한하여 접수업무를 처리하여야 한다.

6.2.2 [P1] 전송목록파일 전송 세부 흐름도

그림 19는 전자기록물 전송 절차 중 하나인 '전송목록파일 전송'의 세부절차이다. 전송목록파일을 전송하기 위해서는 로그인 과정을 통해 하나의 세션을 생성한 후 전송목록파일을 전송한다.

전송목록파일 전송이 성공되면 '.transferring' 파일을 생성하고, 다음 단계인 '전자기록물파일 전송'절차를 병렬로 수행한다.

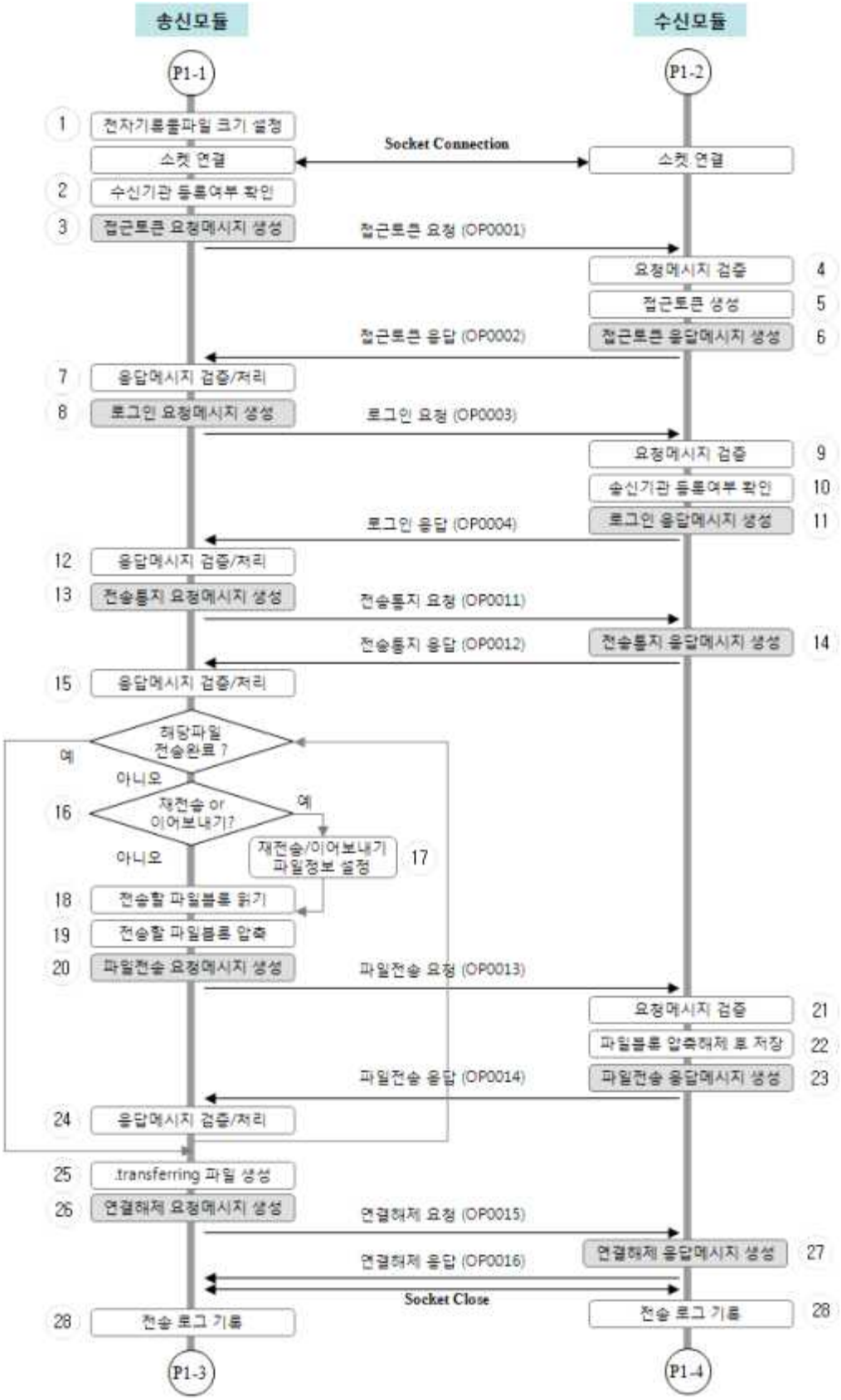

그림 19 - 전송목록파일 전송 세부흐름도

① 전자기록물파일 크기설정
- 송신모듈은 업무시스템에서 생성한 전송목록파일 내의 각 전자기록물 파일크기(file_size)를 설정한다.
- 정상적으로 파일크기 설정이 완료되면 수신모듈로 소켓을 연결한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.
- 해당 기술규격 : '5.2.1 전송목록파일 구조'

② 수신기관 등록여부 확인
- 송신모듈은 별도 관리하는 수신기관의 등록정보를 조회한다.
- 만일 수신모듈의 등록정보가 존재하지 않으면, ③의 로그인 요청메시지에 수신모듈의 등록정보를 요청하여야 한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.

③ 접근토큰 요청메시지 생성
- 송신모듈은 접근토큰 요청메시지를 생성한다.
- '접근토큰 요청'관련 재요청 시간 및 횟수는 '6.1.2 로그인 절차'를 참조한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.
- 세부적인 내용은 '6.3.4.1 접근토큰 요청 (OP0001)'을 참조한다.

④ 요청메시지 검증
- 수신모듈은 송신모듈의 접근토큰 요청메시지를 검증한다.
- 오류 발생 시 '⑥ 접근토큰 응답메시지'에 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.1 접근토큰 요청 (OP0001)'을 참조한다.

⑤ 접근토큰 생성
- 수신모듈은 송신모듈에게 전송할 접근토큰을 생성한다.

⑥ 접근토큰 응답메시지 생성
- 수신모듈은 접근토큰 응답메시지를 생성하여 전달한다.
- 오류 발생 시 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.2 접근토큰 응답 (OP0002)'를 참조한다.

⑦ 응답메시지 검증/처리
- 송신모듈은 수신한 접근토큰 응답메시지를 검증한 후, 로그인 요청메

시지를 생성하며, 로그인 완료시 접속토큰은 전자기록물 전송완료 시까지 유지되어야 한다.

- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.
- 세부적인 내용은 '6.3.4.2 접속토큰 응답 (OP0002)'를 참조한다.

⑧ 로그인 요청메시지 생성

- 송신모듈은 수신모듈에 로그인하기 위해 로그인 요청메시지를 생성한다.
- '로그인 요청'관련 재요청 시간 및 횟수는 '6.1.2 로그인 절차'를 참조한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.
- 세부적인 내용은 '6.3.4.3 로그인 요청 (OP0003)'을 참조한다.

⑨ 요청메시지 검증

- 수신모듈은 송신모듈의 로그인 요청메시지를 검증한다.
- 오류 발생 시 '⑪ 로그인 응답메시지'에 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.3 로그인 요청 (OP0003)'을 참조한다.

⑩ 송신기관 등록여부 확인

- 수신모듈은 송신모듈의 등록여부를 확인한다.
- 등록되지 않았으면 '⑪ 로그인 응답메시지'에 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.

⑪ 로그인 응답메시지 생성

- 수신모듈은 로그인 응답메시지를 생성하여 전달한다.
- 오류 발생 시 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.4 로그인 응답 (OP0004)'를 참조한다.

⑫ 응답메시지 검증/처리

- 송신모듈은 수신한 로그인 응답메시지를 검증한 후, 송신모듈의 등록정보가 존재 시 등록정보를 별도 저장한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.
- 세부적인 내용은 '6.3.4.4 로그인 응답 (OP0004)'를 참조한다.

⑬ 전송통지 요청메시지 생성

- 송신모듈은 해당 전송목록파일 전송을 위한 통지 요청메시지를 생성

한다.

- ’전송통지 요청’관련 재요청 시간 및 횟수는 ’6.1.3 파일전송 시작통지 절차’를 참조한다.
- 통신오류 이외의 오류 발생 시 ‘5.2.2 전송목록파일 관리방안’의 ‘.error’ 파일을 처리하고, 절차 ㉖으로 이동한다.
- 통신오류 발생 시 ‘5.2.2 전송목록파일 관리방안’의 ‘.error’ 파일을 처리한 후, 절차 ㉘로 이동한다.
- 세부적인 내용은 ’6.3.4.7 전송통지 요청 (OP0011)’을 참조한다.

⑭ 전송통지 응답메시지 생성

- 수신모듈은 수신한 전송통지 요청메시지를 검증한 후, 해당 전송통지 응답메시지를 생성한다.
- 수신모듈은 해당 파일에 대해 이미 수신완료한 일부파일이 존재하면 ’currentFileSize’ 필드에 수신한 파일크기를 설정하여 전달한다. 이는 해당 파일에 대해 수신 완료된 이후의 파일블록 ‘이어보내기’를 나타낸다.
- 오류 발생 시, ’연결해제 요청’을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 ’6.3.4.8. 전송통지 응답 (OP0012)’를 참조한다.

⑮ 응답메시지 검증/처리

- 송신모듈은 수신한 전송통지 응답 메시지를 검증한 후, 전송할 파일블록을 계산한다.
- 만일 전송할 파일의 크기가 응답메시지 내의 수신완료 크기 (currentFileSize)보다 작으면 오류 처리한다.
- 만일 전송할 파일의 크기와 응답메시지 내의 수신완료 크기 (currentFile Size)가 같으면 전송완료로 판단한다.
- 오류 발생 시 ’5.2.2 전송목록파일 관리방안’의 ’.error’ 파일을 처리하고, 절차 ㉖으로 이동한다.
- 세부적인 내용은 ’6.3.4.8. 전송통지 응답 (OP0012)’를 참조한다.

⑯ 재전송 또는 이어보내기 판단

- 만일 이 절차가 ’⑮ 전송통지 응답메시지’ 수신 후 처리이고, 전송통지 응답메시지 내 ’currentFileSize’ 값이 1보다 크거나 같고 전송할 파일크기보다 작으면 해당 파일의 일부만 수신된 경우이므로 ’currentFileSize’ 이후의 파일블록을 ‘이어보내기’한다.
- 만일 이 절차가 ’㉔ 파일전송 응답메시지’ 수신 후 처리이고, 파일전송 응답메시지 내 reSendReqCount가 1보다 크고, c_5(’6.1.4 파일전송

절차’ 참조)보다 작으면 해당 파일블록을 재전송하여야 한다. 만일 reSendReqCount가 0이면 정상적으로 다음 파일블록 전송을 나타내고, c_5보다 크면 오류 처리한다.

- 오류 발생 시 ’5.2.2 전송목록파일 관리방안’의 ’.error’ 파일을 처리하고, 절차 ㉖으로 이동한다.

⑰ 재전송 및 이어보내기 파일정보 설정

- 만일 이 절차가 ’⑮ 전송통지 응답메시지’ 수신 후 처리이면, 재전송 및 이어보내기할 파일명은 respNotiMessage.fileName 이고, 전송할 파일블록은 respNotiMessage.currentFileSize로 설정한다.
- 만일 이 절차가 ‘파일전송 응답메시지’ 수신 후 처리이면, 전송할 파일명은 respFileTranferMessage.fileName이고, 전송할 파일블록은 respFileTranferMessage.totalFileSize로 설정한다.

⑱ 전송할 파일블록 읽기

- 만일 이 절차가 ’⑮ 전송통지 응답메시지 검증/처리’ 직후에 이루어지면, 송신모듈은 해당 전송 목록파일에 대하여, ’전송통지 응답메시지’ 내에 기입된 수신완료(currentFileSize) 이후의 파일블록을 읽는다.
- 만일 이 절차가 ’㉔ 응답메시지 검증/처리’ 직후에 이루어지면, ‘파일전송 응답메시지’ 내에 기입된 totalFileSize 이후의 파일블록을 읽는다.
- 오류 발생 시 절차 ⑳으로 이동하여 오류내역을 처리한다.
- 세부적인 내용은 ’6.3.4.9 파일전송 요청 (OP0013)’을 참조한다.

⑲ 전송할 파일블록 압축

- 송신모듈은 전송할 전송목록파일의 파일블록을 압축한다.
- 오류 발생 시 절차 ⑳으로 이동하여 오류내역을 처리한다.
- 세부적인 내용은 ’6.3.4.9 파일전송 요청 (OP0013)’을 참조한다.

⑳ 파일전송 요청메시지 생성

- 송신모듈은 파일블록에 대한 파일전송 요청메시지를 생성한다.
- ’파일전송 요청’ 관련 재요청 시간 및 횟수는 ’6.1.4 파일전송 절차’를 참조한다.
- 통신오류 이외의 오류 발생 시 ’5.2.2 전송목록파일 관리방안’의 ’.error’ 파일을 처리하고, 오류에 대한 요청메시지를 생성하여 수신모듈에 전달한 후, 절차 ㉖으로 이동한다. 오류에 대한 요청메시지를 생성하여 수신모듈에 전달 시, 수신모듈의 응답메시지를 수신하지 않는다.
- 통신오류 발생 시 ’5.2.2 전송목록파일 관리방안’의 ’.error’ 파일을 처

리한 후, 절차 ㉘로 이동한다.

- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

㉑ 요청메시지 검증

- 수신모듈은 파일전송 요청메시지에 대해 검증한다.
- 만일 '파일전송 요청메시지'가 수신모듈의 파일블록 재전송(응답메시지 내 reSendReqCount가 1이상의 값 설정)에 대한 것이면, 요청한 파일블록(respFileTranferMessage.totalFileSize)과 수신한 파일블록(reqFileTransferMessage.curFilePosition)이 일치하는지 검사한다. 일치하지 않으면 c_5 횟수만큼 '㉓ 파일전송 응답메시지 생성'으로 이동하여 송신모듈이 해당 파일블록을 재전송하도록 하고, 일치하면 '㉒ 수신한 파일블록 저장'을 수행한다.
- 만일 reSendReqCount가 c_5 횟수에 도달하면 오류 처리한다.
- 요청메시지가 오류내역을 포함한 메시지이면, 수신모듈은 해당 오류내역을 '.error'에 기입한 후, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 오류 발생 시 '㉓ 파일전송 응답메시지'에 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗이후를 수행한다.
- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

㉒ 수신한 파일블록 압축해제 후 저장

- 수신모듈은 파일전송 요청메시지 내의 파일블록을 저장한다. 만일 파일블록이 압축되어 있으면 압축을 해제하여 저장하여야 한다.
- 오류 발생 시 '㉓ 파일전송 응답메시지'에 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

㉓ 파일전송 응답메시지 생성

- 수신모듈은 파일전송요청에 대한 응답메시지를 생성한다.
- 만일 송신모듈이 해당 파일블록을 재전송하여야 한다면, reSendReqCount를 1 증가하고, 재전송할 파일블록(respFileTranferMessage.totalFileSize)을 기입한 파일전송 응답메시지를 생성한다.
- 오류 발생 시, '연결해제 요청'을 대기하여 절차 ㉗ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.10 파일전송 응답 (OP0014)'를 참조한다.

㉔ 응답메시지 검증/처리

- 송신모듈은 파일전송 응답메시지에 대해 검증을 수행한 후, 해당 파일에 대해 전송할 블록이 남아있는 경우 ⑯~㉔를 반복 수행한다.

- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ㉖으로 이동한다.
- 세부적인 내용은 '6.3.4.10 파일전송 응답 (OP0014)'를 참조한다.

㉕ .transferring 파일생성
- 송신모듈은 해당 전송목록파일 내 기술된 전자기록물파일 전송시작을 나타내는 '.transferring' 파일을 생성한다.
- 해당 기술규격 : '5.2.2 전송목록파일 관리방안'

㉖ 연결해제 요청메시지 생성
- 송신모듈은 소켓종료를 위한 연결해제 요청메시지를 생성한다.
- 오류 발생 시, 소켓을 종료한다.
- 세부적인 내용은 '6.3.4.11 연결해제 요청 (OP0015)'를 참조한다.

㉗ 연결해제 응답메시지 생성
- 수신모듈은 연결해제 요청에 대한 응답메시지를 생성한다.
- 연결해제 응답메시지 전송 후, 사용한 자원 반납처리를 수행하고 소켓을 종료한다.
- 오류 발생 시, 소켓을 종료한다.
- 세부적인 내용은 '6.3.4.12 연결해제 응답 (OP0016)'을 참조한다.

㉘ 전송로그 기록
- 전송내역에 대한 정보는 '6.4.1 모니터링을 위한 로그포맷'에서 정의한 형식을 준용하여 로그파일로 기록한다.
- 오류 발생 시 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에서 정의된 형식을 준용하여 로그파일로 기록한다. 이때, 동일 오류내역이 중복으로 기입되지 않도록 한다.
- 오류 발생 시, 로그인 정보는 초기화되어야 하고, '접근토큰' 값도 더 이상 유지되어서는 안 된다.

6.2.3 [P2] 전자기록물파일 전송 세부 흐름도

그림 20은 '전송목록파일 전송' 이후 수행되는 '전자기록물파일 전송'의 세부 절차이다. 전자기록물파일을 전송하기 위해서는 하나의 세션을 생성한 후 전자기록물파일을 전송한다.

생성된 하나의 세션을 이용하여 다수의 전자기록물파일들을 보낼 수 있다(다중파일 전송). 이 '전자기록물파일 전송'은 병렬로 수행(다중세션전송)될 수

있고, 모든 전자기록물파일이 전송 완료되면 다음 단계인 '전송목록파일 전송완료 통보' 절차를 수행한다.

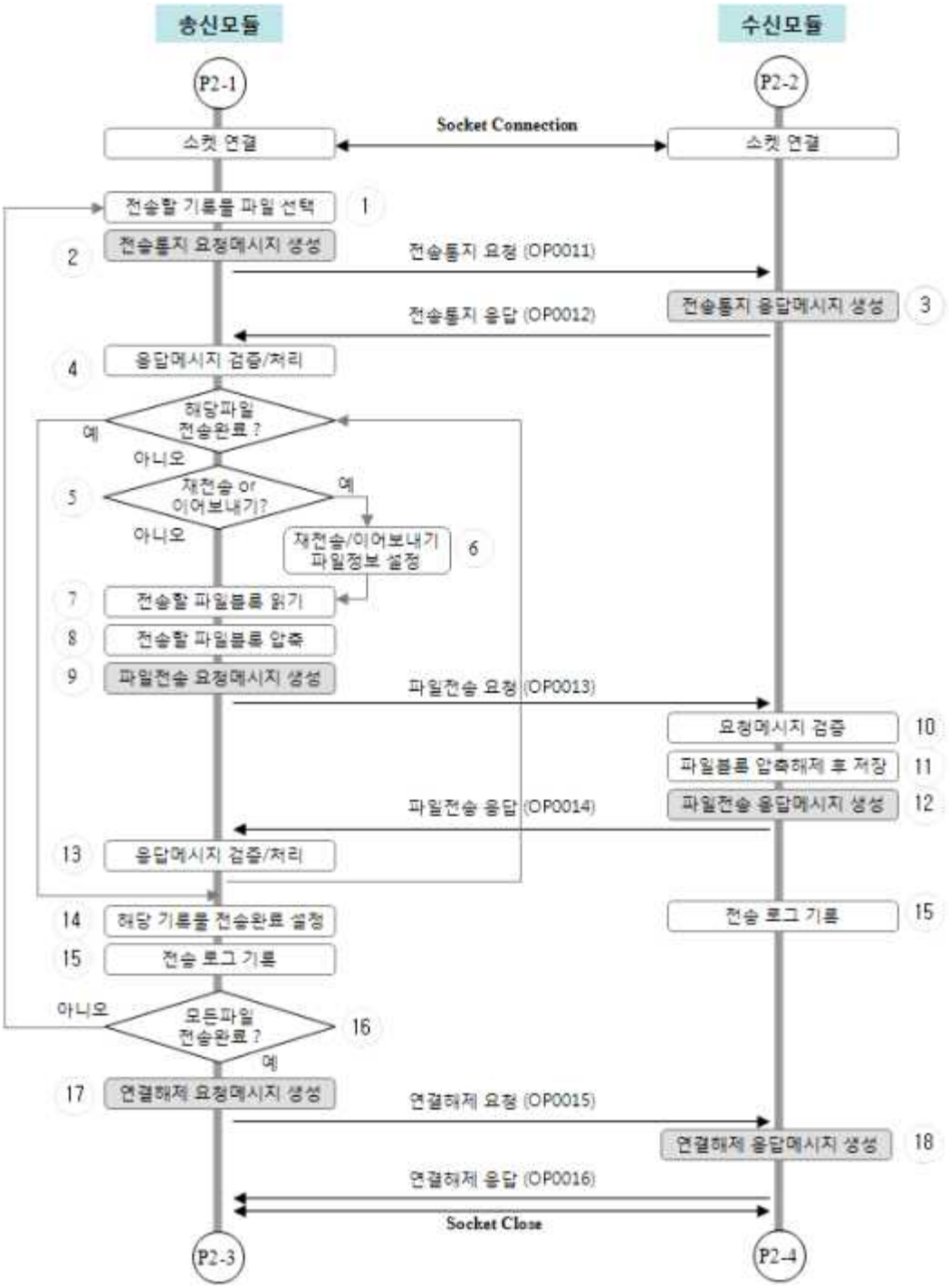

그림 20 - 전자기록물파일 전송 세부 흐름도

① 전송할 전자기록물파일 선택

- 전송목록파일에 기술된 전자기록물파일들 중 하나의 파일을 선택한다.
- 전송할 전자기록물파일은 현 쓰레드(또는 프로세스)에 할당된 전자기록물 파일들 중 전송이 완료되지 않은 하나의 전자기록물파일을 의미한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리한 후, 절차 ⑮로 이동한다.

② 전송통지 요청메시지 생성

- 송신모듈은 해당 전자기록물파일 전송을 위한 통지 요청메시지를 생성한다.
- '전송통지 요청'관련 재요청 시간 및 횟수는 '6.1.3 파일전송 시작통지 절차'를 참조한다.
- 통신오류 이외의 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리한 후, 절차 ⑮로 이동한다.
- 통신오류 발생시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리한 후, 절차 ⑰로 이동한다.
- 세부적인 내용은 '6.3.4.7 전송통지 요청 (OP0011)'을 참조한다.

③ 전송통지 응답메시지 생성

- 수신모듈은 수신한 전송통지 요청메시지를 검증한 후, 해당 전송통지 응답메시지를 생성한다.
- 수신모듈은 해당 파일에 대해 이미 수신완료한 일부파일이 존재하면 'currentFileSize' 필드에 수신한 파일크기를 설정하여 전달한다. 이는 해당 파일에 대해 수신 완료된 이후의 파일블록 '이어보내기'글 나타낸다.
- 오류 발생 시, 절차 ⑮로 이동한다.
- 세부적인 내용은 '6.3.4.8. 전송통지 응답 (OP0012)'를 참조한다.

④ 응답메시지 검증/처리

- 송신모듈은 수신한 전송통지 응답메시지를 검증한 후, 전송할 파일블록을 계산한다.
- 만일 전송할 파일의 크기가 응답메시지 내의 수신완료 크기(current FileSize)보다 작으면 오류 처리한다.
- 만일 전송할 파일의 크기와 응답메시지 내의 수신완료 크기(current File Size)가 같으면 전송완료로 판단한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ⑮로 이동한다.

- 세부적인 내용은 '6.3.4.8. 전송통지 응답 (OP0012)'를 참조한다.

⑤ 재전송 또는 이어보내기 판단

- '전송통지 응답메시지' 수신 후 처리이고 해당 파일에 대한 is_resend 값이 '1'인 경우, 전송통지 응답메시지 내 'currentFileSize' 값과 무관하게 해당 파일을 '재전송'한다.
- '전송통지 응답메시지' 수신 후 처리이고 해당 파일에 대한 is_resend 값이 '0'인 경우, 전송통지 응답메시지 내 'currentFileSize' 값이 1보다 크거나 같고 전송할 파일크기보다 작으면 해당 파일의 일부만 수신된 경우이므로 'currentFileSize' 이후의 파일블록을 '이어보내기'한다.
- 만일 이 절차가 '파일전송 응답메시지' 수신 후 처리이고, 파일전송 응답메시지 내 reSendReqCount가 1보다 크고 c_5('6.1.4 파일전송 절차' 참조)보다 작으면 해당 파일블록을 재전송하여야 한다. 만일 reSendReqCount가 0이면 정상적으로 다음 파일블록 전송을 나타내고, c_5보다 크면 오류 처리한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ⑮로 이동한다.

⑥ 재전송 및 이어보내기 파일정보 설정

- 만일 이 절차가 '전송통지 응답메시지' 수신 후 처리이면, 재전송 및 이어보내기할 파일명은 respNotiMessage.fileName 이고, 전송할 파일블록은 respNotiMessage.currentFileSize로 설정한다.
- 만일 이 절차가 '파일전송 응답메시지' 수신 후 처리이면 respFileTranferMessage.fileName이고, 전송할 파일블록은 respFileTranferMessage.totalFileSize로 설정한다.

⑦ 전송할 파일블록 읽기

- 만일 이 절차가 '④ 응답메시지 검증/처리' 직후에 이루어지면, 송신모듈은 해당 전자기록물파일에 대해 '전송통지 응답메시지' 내에 기입된 수신완료(currentFileSize) 이후의 파일블록을 읽는다.
- 만일 이 절차가 '⑬ 응답메시지 검증/처리' 직후에 이루어지면, '파일전송 응답메시지' 내에 기입된 totalFileSize 이후의 파일블록을 읽는다.
- 오류 발생 시, 절차 ⑨로 이동하여 오류내역을 처리한다.
- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

⑧ 전송할 파일블록 압축

- 송신모듈은 전송할 전자기록물파일에 대해, 전송목록파일 내에 압축여부(tb_compressed)가 'true'이면 파일블록을 압축한다. 만일 'false'이면

압축단계는 생략한다.

- 오류 발생 시 절차 ⑨로 이동하여 오류내역을 처리한다.
- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

⑨ 파일전송 요청메시지 생성

- 송신모듈은 파일전송 요청메시지를 생성한다.
- '파일전송 요청'관련 재요청 시간 및 횟수는 '6.1.4 파일전송 절차'를 참조한다.
- 통신오류 이외의 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고 오류에 대한 요청메시지를 생성하여 수신모듈에 전달한 후 절차 ⑮로 이동한다.

⑩ 요청메시지 검증

- 수신모듈은 파일전송 요청메시지에 대하여 검증한다.
- 만일 '파일전송 요청메시지'가 수신모듈의 파일블록 재전송(응답메시지 내 reSendReqCount가 1 이상의 값 설정)에 대한 것이면, 요청한 파일블록(respFileTranferMessage.totalFileSize)과 수신한 파일블록(reqFileTransferMessage.curFilePosition)이 일치하는지 검사한다. 일치하지 않으면 c_5 횟수만큼 '⑫ 파일전송 응답메시지 생성'으로 이동하여 송신모듈이 해당 파일블록을 재전송하도록 하고, 일치하면 '⑪ 수신한 파일블록 저장'을 수행한다.
- 만일 reSendReqCount가 c_5 횟수에 도달하면 오류 처리한다.
- 요청메시지가 오류내역을 포함한 메시지이면, 수신모듈은 해당 오류내역을 '.error'에 기입한 후, 절차 ⑮로 이동한다.
- 오류 발생 시 '⑫ 파일전송 응답메시지'에 해당 오류메시지를 전달한 후에 절차 ⑮로 이동한다.
- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

⑪ 수신한 파일블록 저장

- 수신모듈은 파일전송 요청메시지 내의 파일블록을 저장한다. 만일 파일블록이 압축되어 있으면 압축을 해제하여 저장하여야 한다.
- 오류 발생 시 '⑫ 파일전송 응답메시지'에 해당 오류메시지를 전달한 후에 절차 ⑮로 이동한다.
- 세부적인 내용은 '6.3.4.9 파일전송 요청 (OP0013)'을 참조한다.

⑫ 파일전송 응답메시지 생성

- 수신모듈은 파일전송요청에 대한 응답메시지를 생성한다.
- 만일 송신모듈이 해당 파일블록을 재전송하여야 한다면, reSendReqC

ount를 1 증가하고, 재전송할 파일블록(respFileTranferMessage.totalFileSize)을 기입한 파일전송 응답메시지를 생성한다.

- 오류 발생 시 절차 ⑮로 이동한다.
- 세부적인 내용은 '6.3.4.10 파일전송 응답 (OP0014)'를 참조한다.

⑬ 응답메시지 검증/처리

- reSendReqCount가 0이면, 이후 전송할 파일블록이 존재하는지 확인한다.
- 송신모듈은 파일전송 응답메시지를 검증한 후, 해당 파일에 대해 전송할 파일블록이 남아있는 경우 ⑤~⑬을 반복 수행한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리한 후에 절차 ⑮로 이동한다.
- 세부적인 내용은 '6.3.4.10 파일전송 응답 (OP0014)'를 참조한다.

⑭ 해당 전자기록물 전송완료 설정

- 송신모듈은 전송 완료된 전자기록물파일에 대해, 전송목록파일 내 is_transfered 필드를 '1'로 변경하여 전송완료를 설정한다.
- 해당 기술규격 : '5.2.1 전송목록파일 구조'

⑮ 전송로그 기록

- 전송내역에 대한 정보는 '6.4.1 모니터링을 위한 로그포맷'에서 정의한 형식을 준용하여 로그파일로 기록한다.
- 오류 발생 시 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에서 정의된 형식을 준용하여 로그파일로 기록한다. 이때, 동일 오류내역이 중복으로 기입되지 않도록 한다.

⑯ 모든 전자기록물파일 전송완료 여부 확인

- 현재의 쓰레드(또는 프로세스)에 할당된 모든 전자기록물파일의 전송완료 여부를 확인한다.
- 현재의 쓰레드(또는 프로세스)는 초기 연결된 하나의 세션을 이용하여 할당된 모든 전자기록물파일들을 전송하는 '다중파일 전송'을 수행한다.
- 다중파일 전송이 완료되면 세션을 종료하고, 그렇지 않은 경우에는 ① ~ ⑯ 절차를 반복 수행한다.

⑰ 연결해제 요청메시지 생성

- 송신모듈은 소켓종료를 위한 연결해제 요청메시지를 생성한다.
- 오류 발생 시, 소켓을 종료한다.
- 세부적인 내용은 '6.3.4.11 연결해제 요청 (OP0015)'를 참조한다.

⑱ 연결해제 응답메시지 생성

- 수신모듈은 연결해제 요청에 대한 응답메시지를 생성한다.
- 연결해제 응답메시지 전송 후, 사용한 자원의 반납처리를 수행한 다음 소켓을 종료한다.
- 오류 발생 시 소켓을 종료한다.
- 세부적인 내용은 '6.3.4.12 연결해제 응답 (OP0016)'을 참조한다.

6.2.4 [P3] 전송목록파일 전송완료 통보 세부 흐름도

그림 21은 모든 '전자기록물파일 전송'이 완료된 이후 수행되는 '전송목록파일 전송완료 통보'의 세부절차이다. 전송완료 통보를 전송하기 위해서는 하나의 세션을 생성한 후 전송목록파일에 대한 전자기록물 전송완료를 통보한다.

수신모듈은 송신모듈의 전송완료를 통보하는 '전송통지 요청' 메시지를 수신하면 파일 일치성 검사를 수행해야 한다. 파일 일치성 검사를 위해서는 'P1 전송목록파일 전송' 절차에서 수신한 전송목록파일과 'P2 전자기록물파일 전송' 절차에서 수신한 전자기록물파일들이 필요하다. 이 절차에서 수행된 파일 일치성 검사가 성공하면 이후 절차인 '시점확인토큰 생성'을 수행한다.

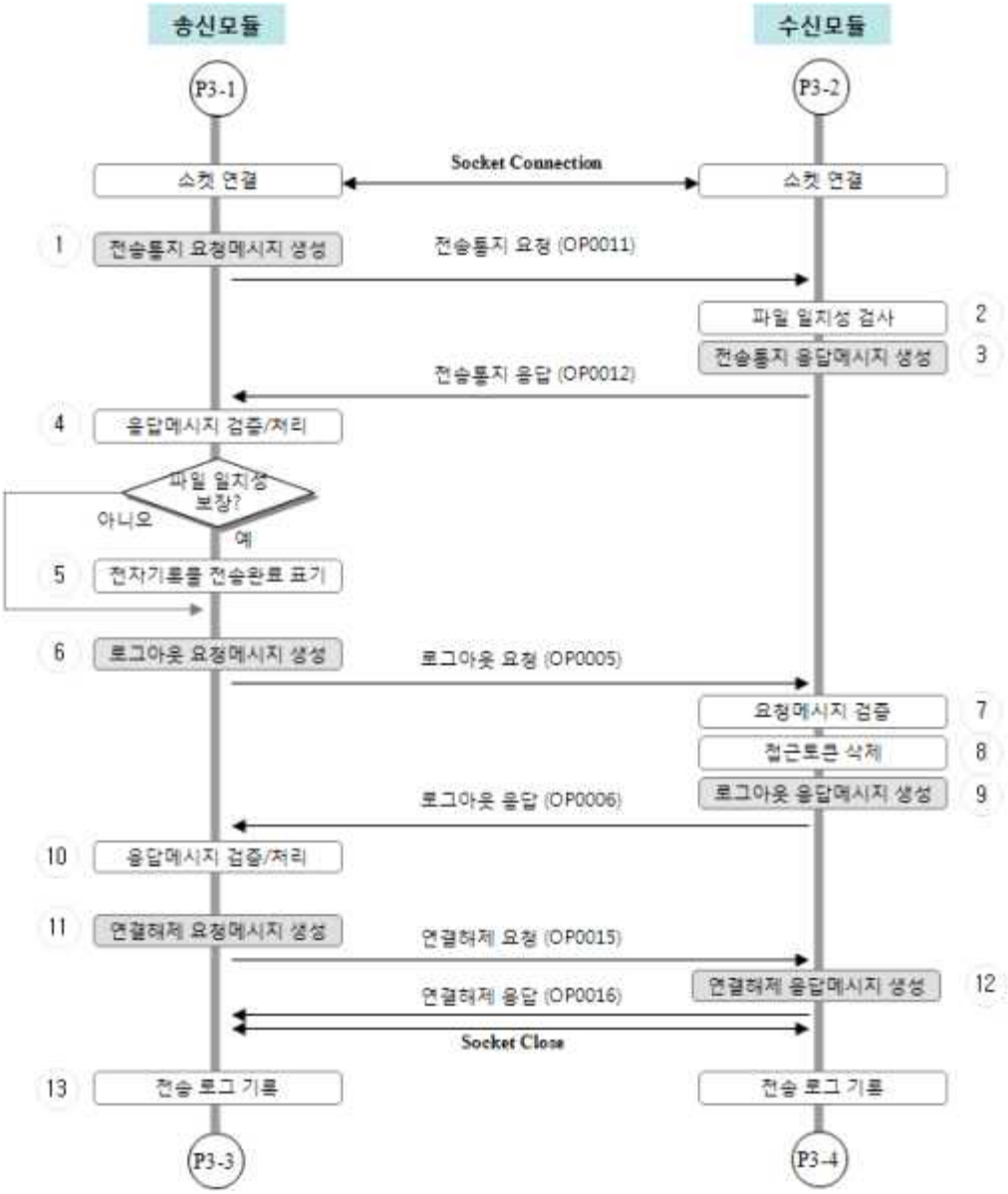

그림 21 - 전송목록파일 전송완료 통보 세부 흐름도

① 전송통지 요청메시지 생성

- 송신모듈은 해당 전송목록파일 전송을 위한 통지 요청메시지를 생성한다.
- '전송통지 요청'관련 재요청 시간 및 횟수는 '6.1.5 파일전송 완료통지 절차'를 참조한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ⑥으로 이동한다.
- 세부적인 내용은 '6.3.4.7 전송통지 요청 (OP0011)'을 참조한다.

② 파일 일치성 검사

- 수신모듈은 해당 전송목록파일에 대한 파일 일치성 검사를 수행한다. 파일 일치성이 보장되지 않으면 해당 전송목록파일에 대해 시점확인 토큰 생성 및 업무시스템의 접수처리 기능 호출 절차가 수행되지 않아야 한다.
- 수신모듈은 파일 일치성이 보장된 경우에 한하여 '.end' 파일을 생성하여야 한다.
- 파일 일치성 검사는 'P1 전송목록파일 전송' 절차에서 수신한 '전송목록파일'과 'P2 전자기록물파일 전송' 절차에서 수신한 전자기록물파일들을 이용하여 파일리스트 및 각 파일들의 크기 비교를 수행하여야 한다.
- 오류 발생 시 '③ 전송통지 응답메시지'에 해당 오류메시지를 전달하고, '로그아웃 요청'을 대기하여 절차 ⑫ 이후를 수행한다.
- 파일 일치성 검사는 '4.2 기능 요구사항'의 '4.2.6 파일 일치성 보장'을 참조한다.

③ 전송통지 응답메시지 생성

- 수신모듈은 수신한 전송통지 요청메시지를 검증한 후, 해당 전송통지 응답메시지를 생성한다.
- 오류 발생 시, '로그아웃 요청'을 대기하여 절차 ⑫ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.8 전송통지 응답 (OP0012)'를 참조한다.

④ 요청메시지 검증/처리

- 송신모듈은 수신한 전송통지 응답메시지를 검증한다.
- 오류 발생 시, 절차 ⑥으로 이동한다.
- 세부적인 내용은 '6.3.4.4 전송통지 응답 (OP0012)'를 참조한다.

⑤ 전자기록물 전송완료 표기

- 본 절차는 수신모듈의 파일 일치성 검사가 성공한 경우에 한해 수행되어야 한다.
- 해당 전송목록파일에 대한 전송시작 표기파일(.transferring)을 삭제한 후, 전송완료(.complete) 파일을 생성한다.
- 송신모듈은 전송이 성공적으로 완료된 전송목록파일(.xml) 및 관련 파일들(.end, .complete) 그리고 해당 전자기록물파일을 'sendcomplete' 디렉토리로 이동시켜야 한다.
- 업무시스템은 해당 전송목록파일에 대한 전송완료를 식별할 수 있다.
- 해당 기술규격 : '5.2.2 전송목록파일 관리방안'

⑥ 로그아웃 요청메시지 생성

- 송신모듈은 수신모듈에 로그아웃하기 위해 로그아웃 요청메시지를 생성한다.
- '로그아웃 요청'관련 재요청 시간 및 횟수는 '6.1.6 로그아웃 절차'를 참조한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ⑪로 이동한다.
- 세부적인 내용은 '6.3.4.5 로그아웃 요청 (OP0005)'를 참조한다.

⑦ 요청메시지 검증

- 수신모듈은 송신모듈의 로그아웃 요청메시지를 검증한다.
- 오류 발생 시 '⑨ 로그아웃 응답메시지'에 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ⑫이후를 수행한다.
- 세부적인 내용은 '6.3.4.5 로그아웃 요청 (OP0005)'를 참조한다.

⑧ 접근토큰 삭제

- 수신모듈은 송신모듈과 공유한 접근토큰을 삭제한다. 이후 송신모듈은 동일한 접근토큰을 사용하여 세션을 생성할 수 없고, 새로운 로그인과정을 거쳐 접근토큰을 생성하여야 한다.

⑨ 로그아웃 응답메시지 생성

- 수신모듈은 로그아웃 응답메시지를 생성하여 전달한다.
- 오류 발생 시 해당 오류메시지를 전달하고, '연결해제 요청'을 대기하여 절차 ⑫ 이후를 수행한다.
- 세부적인 내용은 '6.3.4.6 로그아웃 응답 (OP0006)'을 참조한다.

⑩ 응답메시지 검증/처리

- 송신모듈은 수신한 로그아웃 응답메시지를 검증한 후, 공유한 접근토큰을 삭제한다. 이후 송신모듈은 동일한 접근토큰을 사용하여 세션을 생성할 수 없고, 새로운 로그인과정을 거쳐 접근토큰을 생성해야 한다.
- 오류 발생 시 '5.2.2 전송목록파일 관리방안'의 '.error' 파일을 처리하고, 절차 ⑪로 이동한다.
- 세부적인 내용은 '6.3.4.6 로그아웃 응답 (OP0006)'을 참조한다.

⑪ 연결해제 요청메시지 생성

- 송신모듈은 소켓종료를 위한 연결해제 요청메시지를 생성한다.
- 오류 발생 시, 소켓을 종료한다.
- 세부적인 내용은 '6.3.4.11 연결해제 요청 (OP0015)'를 참조한다.

⑫ 연결해제 응답메시지 생성

- 수신모듈은 연결해제 요청에 대한 응답메시지를 생성한다.
- 연결해제 응답메시지 전송 후, 사용한 자원을 반납처리 수행하고 소켓을 종료한다.
- 오류 발생 시, 소켓을 종료한다.
- 세부적인 내용은 '6.3.4.12 연결해제 응답 (OP0016)'을 참조한다.

⑬ 전송로그 기록

- 전송내역에 대한 정보는 '6.4.1 모니터링을 위한 로그포맷'에서 정의한 형식을 준용하여 로그파일로 기록한다.
- 오류 발생 시 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에서 정의된 형식을 준용하여 로그파일로 기록한다.

6.2.5 [P4] 시점확인토큰 생성 세부 흐름도

그림 22는 '전송목록파일 전송완료 통보' 후 파일 일치성 검사가 모두 성공한 경우에 한해 수신모듈에서만 수행하는 '시점확인토큰 생성' 세부절차이다.

이 절차에서는 전송이 완료된 현 전송목록파일뿐만 아니라, 이전에 전송 완료된 목록파일 중 시점확인 토큰을 생성하지 못한 전송목록파일까지 모두 시점확인 토큰을 생성한다.

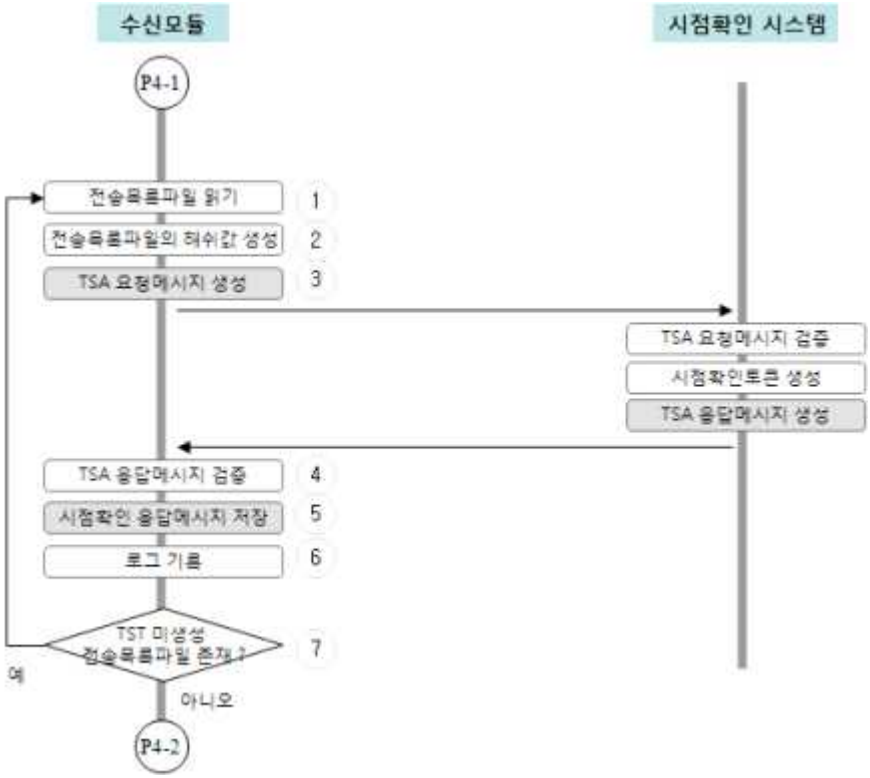

그림 22 - 시점확인토큰 생성 세부 흐름도

① 전송목록파일 읽기

- 수신모듈은 전송이 완료된 전송목록파일을 읽는다.
- 에러 발생 시 절차 ⑥으로 이동한다.

② 전송목록파일의 해쉬값 생성

- SHA-1 해쉬알고리즘을 이용하여 전송목록파일의 해쉬값을 생성한다.
- 에러 발생 시 절차 ⑥으로 이동한다.

③ TSA 요청메시지 생성

- 생성된 해쉬값을 이용하여 시점확인 토큰 요청메시지를 생성한다.
- 'TSA 요청'관련 재요청 횟수는 3회로 하고, 타임아웃은 시점확인 시스템에서 정의한 값을 사용하되 기본은 30초로 한다.
- 에러 발생 시 절차 ⑥으로 이동한다.
- TSA 요청메시지는 'RFC 3161' 표준을 준용한다. (참고문헌 [3])

④ TSA 응답메시지 검증

- 시점확인 토큰을 포함한 TSA 응답메시지를 검증한다.
- 에러 발생 시 절차 ⑥으로 이동한다.
- TSA 응답메지지 검증은 'RFC 3161' 표준을 준용한다. (참고문헌 [3])

⑤ 시점확인 응답메시지 저장

- 시점확인 토큰을 포함한 시점확인 응답메시지를 '.tst' 확장자로 저장한다.
- 해당 기술규격 : '5.2.2 전송목록파일 관리방안'

⑥ 로그 기록

- 오류 발생 시 오류내역은 '6.4.2 오류내역을 위한 로그포맷'에서 정의된 형식을 준용하여 로그파일로 기록한다.

⑦ TST 미생성 전송목록파일 존재 확인

- 파일 일치성 검사를 수행했으나 시점확인 토큰 정보를 생성하지 못한 전송목록파일이 존재하는지 확인한다.
- TST 미생성 전송목록파일은 '.end'가 존재하고 '.error' 및 '.tst' 파일이 존재하지 않은 파일을 나타낸다.

6.3 메시지 규격

6.3.1 메시지 표현방식

메시지 표현방식은 가상 및 전송구문의 표준인 ASN.1(abstract syntax notation number one)을 이용하고 메시지 교환은 ASN.1 바이너리 교환형식을 준용하여야 한다.

6.3.2 통신 프로토콜

데이터 전송 프로토콜은 TCP/IP 소켓 방식을 이용하여 별도 정의된 패킷을 구성하여 전송해야 한다. 패킷은 고정부와 가변부로 구성된다. 고정부는 가변의 길이를 나타내고, 가변부(content)는 송·수신 메시지를 포함하여야 한다.

요청/응답 패킷의 기본 구성은 다음과 같다.

고정부 (Length: 4Byte)	가변부 (Content)
Content의 Length	ARCTRRequest/ARCTRResponse (송·수신 메시지)

비고 고정부(length)는 Big-Endian network order를 따라야 한다.

6.3.3 송·수신 메시지 구성

송·수신 메시지는 ASN.1 형식을 이용하여 표현되고, DER 인코딩되어야 한다.

·송·수신 메시지 : = DER_Encoding {송·수신 메시지정보}

송·수신 메시지 종류는 표 8과 같다.

표 8 - 송·수신 메시지 종류

메시지 종류	메시지 이름	설 명
OP0001	접근토큰 요청	로그인을 위한 접근토큰 요청메시지
OP0002	접근토큰 응답	로그인을 위한 접근토큰 응답메시지
OP0003	로그인 요청	로그인 요청을 위한 메시지
OP0004	로그인 응답	로그인 처리결과 응답메시지
OP0005	로그아웃 요청	로그아웃 요청을 위한 메시지
OP0006	로그아웃 응답	로그아웃 처리결과 응답메시지
OP0011	전송통지 요청	파일의 기본정보 상호검사 요청메시지
OP0012	전송통지 응답	파일의 기본정보 상호검사 응답메시지
OP0013	파일전송 요청	전송할 파일정보를 포함한 요청메시지
OP0014	파일전송 응답	수신한 파일정보 처리결과 응답메시지
OP0015	연결해제 요청	연결중인 소켓 연결 해제 요청메시지
OP0016	연결해제 응답	연결중인 소켓 연결 해제 응답메시지

6.3.4 송·수신 메시지 세부설계

(a) 요청 메시지

전자기록물을 전송하기 위한 요청문은 Header, Body, 그리고 무결성 정보로 구성되고, Body는 메시지 종류별로 해당 요청메시지 구조를 가져야 한다.

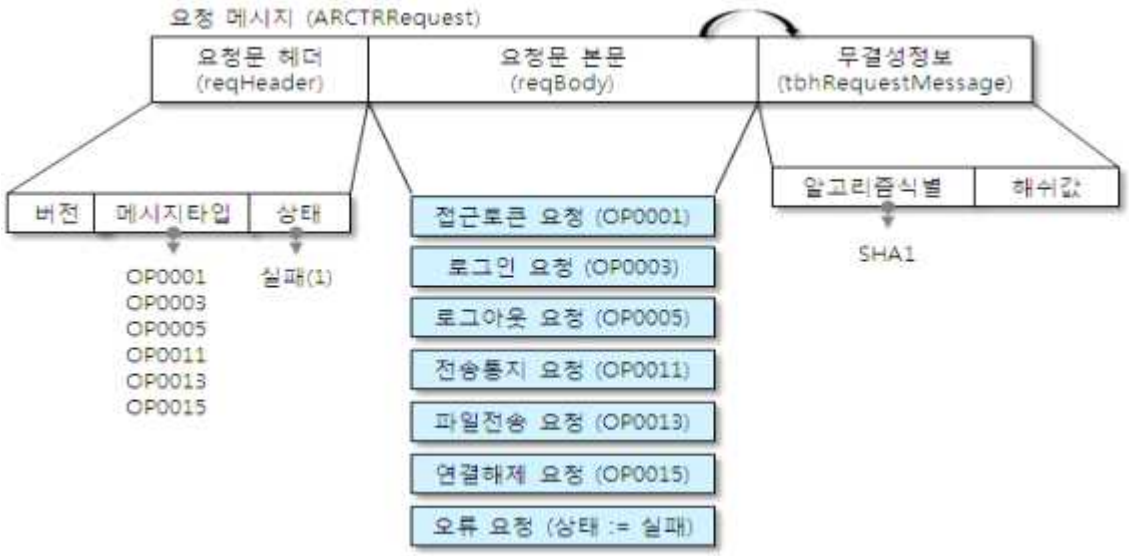

그림 23 - 요청메시지 구조

```
ARCTRRequest ::= SEQUENCE {
        reqHeader           ARCTRHeader
        reqBody             ARCTRRequestMessage,
        tbhRequestMessage   tbhMessage
}
```

- reqHeader는 요청메시지의 헤더를 나타낸다.
- reqBody는 요청메시지의 body 부분으로 메시지 종류별로 '6.3.4.1' 이하에서 기술한 요청메시지의 형식을 가져야 한다.
- tbhRequestMessage는 요청메시지의 body부분인 reqBody에 대한 무결성 정보를 나타낸다. 무결성 정보는 ARCTRRequestMessage의 DER 인코딩된 정보에 대한 해쉬값으로 생성되어야 한다.

```
ARCTRHeader ::= SEQUENCE {
        version             INTEGER,
        optype              OCTET STRING,
        status          [0] ARCTRMessageStatus OPTIONAL
}
```

- version은 요청 및 응답메시지의 버전정보로, '1'을 가져야 한다.
- optype은 요청 및 응답메시지에 대한 구분으로 '6.3.3. 송·수신 메시지 구성'에서 규정한 메시지 종류를 가져야 한다.

- status는 요청 및 응답메시지의 상태값을 나타내는 값으로, 요청메시지는 선택적으로 사용하고, 응답메시지는 필수로 사용하여야 한다.

```
ARCTRMessageStatus ::= ENUMERATED {
        successful      (0),    --성공
        fail            (1)     --실패
}

ARCTRRequestMessage ::= CHOICE {
        orgCode                 OCTET STRING,       -- 접근토큰 요청 (OP0001)
                                                    -- 로그아웃 요청 (OP0005)
                                                    -- 연결해제 요청 (OP0015)
        arctrReqLogin           reqLoginMessage,    -- 로그인 요청 (OP0003)
        arctrReqNoti            reqNotiMessage,     -- 전송통지 요청 (OP0011)
        arctrReqFileTrans       reqFileTransferMessage -- 파일전송 요청 (OP0013)
       errMessage ErrorMessage                      -- 실패에 대한 요청
}
```

- orgCode는 기관코드값으로 '접근토큰 요청메시지', '로그아웃 요청메시지', 그리고 '연결해제 요청메시지'에서 사용된다. 세부적인 형식은 '6.3.4.1 접근토큰 요청 (OP0001)', '6.3.4.5 로그아웃 요청 (OP0005)', '6.3.4.11 연결해제 요청 (OP0015)'에서 기술한다.
- reqLoginMessage는 로그인 요청메시지를 나타낸다. 세부적인 형식은 '6.3.4.3 로그인 요청 (OP0003)'에서 기술한다.
- reqNotiMessage는 전송통지 요청메시지를 나타낸다. 세부적인 형식은 '6.3.4.7 전송통지 요청 (OP0011)'에서 기술한다.
- reqFileTransferMessage는 파일전송 요청메시지를 나타낸다. 세부적인 형식은 '6.3.4.9 파일전송 요청 (OP0013)'에서 기술한다.
- ErrorMessage는 송신모듈이 수신모듈에 오류내역을 통보하기 위해 선택적으로 사용한다. 송신모듈은 요청메시지에 처리 중 오류가 발생하면 errMessage를 통해 오류코드 및 오류메시지를 전달하여야 한다. reqHeader.status가 fail(1)로 설정되어 있으면 reqBody는 errMessage를 가져야 한다.

```
tbhMessage ::= SEQUENCE {
        hashAlgorithm           AlgorithmIdentifier,
```

```
        hashValue               OCTET STRING
}
```

- hashAlgorithm는 해쉬값 생성 시 사용된 해쉬알고리즘의 식별자를 나타낸다. 이 규격에서는 SHA1(1.3.14.3.2.26) 해쉬알고리즘 식별자를 가져야 한다.
- hashValue값은 hashAlgorithm에 의해 생성된 해쉬값으로 바이너리 값이 기술된다. 메시지를 수신한 송·수신모듈은 반드시 메시지 무결성 정보를 검사하여, 무결성 정보 검증이 성공될 때 해당 메시지를 처리하여야 한다.

```
AlgorithmIdentifier ::= SEQUENCE {
        algorithm       OBJECT IDENTIFIER,
        parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

SHA1 OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26 }

(b) 응답 메시지

전자기록물 온라인 전송을 위한 전송기술의 응답문은 Header, Body, 그리고 무결성 정보로 구성되고, Body는 메시지 종류별로 해당 응답메시지 구조를 가져야 한다.

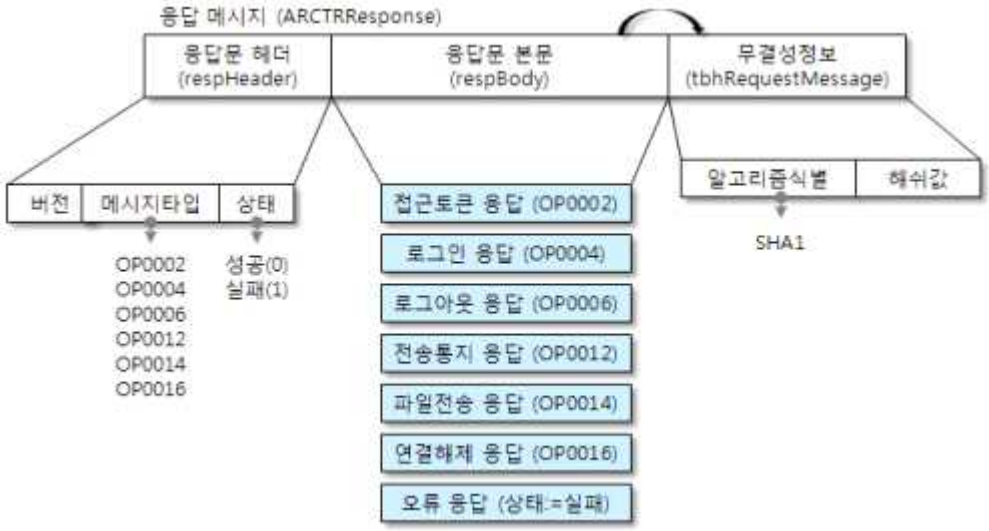

그림 24 - 응답메시지 구조

```
ARCTRResponse ::= SEQUENCE {
        respHeader              ARCTRHeader
        respBody                ARCTRResponseMessage,
        tbhRequestMessage       tbhMessage
}
```

- respHeader는 응답메시지의 헤더를 나타낸다.
- respBody는 응답메시지의 body 부분으로 메시지 종류별로 '6.3.4.1' 이하에서 기술한 응답메시지의 형식을 가져야 한다.
- tbhRequestMessage는 응답메시지의 Body 부분인 respBody에 대한 무결성 정보를 기입한다. 메시지 무결성 정보는 ARCTRResponseMessage의 DER 인코딩된 정보에 대한 해쉬값을 가져야 한다.

```
ARCTRResponseMessage ::= CHOICE {
        arctrRespAccessToken    OCTET STRING,       -- 접근토큰 응답 (OP0002)
        arctrRespLogin          respLoginMessage,   -- 로그인 응답 (OP0004)
        orgCode                 OCTET STRING,       -- 로그아웃 응답 (OP0006)
                                                    -- 연결해제 응답 (OP0016)

        arctrRespNoti           respNotiMessage,    -- 전송통지 응답 (OP0012)
        arctrRespFileTrans      respFileTranferMessage -- 파일전송 응답 (OP0014)
        errMessage              ErrorMessage        -- 실패에 대한 응답
}
```

- orgCode는 기관코드값으로 '접근토큰 응답메시지', '로그아웃 응답메시지', 그리고 '연결해제 응답메시지'에서 사용된다. 세부적인 형식은 '6.3.4.2 접근토큰 응답 (OP0002)', '6.3.4.6 로그아웃 응답 (OP0006)', '6.3.4.12 연결해제 응답 (OP0016)'에서 기술한다.
- respLoginMessage는 로그인 응답메시지를 나타낸다. 세부적인 형식은 '6.3.4.4 로그인 응답 (OP0004)'에서 기술한다.
- respNotiMessage는 전송통지 응답메시지를 나타낸다. 세부적인 형식은 '6.3.4.8 전송통지 응답 (OP0012)'에서 기술한다.
- respFileTranferMessage는 파일전송 응답메시지를 나타낸다. 세부적인 형식은 '6.3.4.10 파일전송 응답 (OP0014)'에서 기술한다.
- ErrorMessage는 오류에 대한 응답메시지를 나타낸다. 수신모듈은 요청메시지에 대한 검증 또는 내부처리 중 오류가 발생하면 errMessage를

통해 오류코드 및 오류메시지를 전달하여야 한다. respHeader.status가 fail(1)로 설정되어 있으면 respBody는 errMessage를 가져야 한다.

```
ErrorMessage ::= SEQUENCE {
        errorCode                   OCTET STRING,
        errorMsgContent     [0]     OCTET STRING OPTIONAL
}
```

- errorCode는 오류코드 값을 나타내며, 하나의 문자(E)에 4자리 정수형을 가진 5자리(EXXXX)로 문자열로 구성되어야 한다.
- errorMsgContent는 오류메시지를 포함한 OCTET STRING을 갖는다. 오류메시지가 존재하지 않은 경우에는 이 필드는 사용되지 않아야 한다.
- 오류코드 및 메시지는 '6.4.2 오류내역을 위한 로그포맷'에 정의한 내용을 가져야 하고, 필요시 추가하여 사용할 수 있다.

6.3.4.1 접근토큰 요청 (OP0001)

접근토큰 요청은 사용자 인증을 위한 선행 절차로, 서버에게 '접근토큰'을 요청한다. 접근토큰은 로그인 처리 시 소유여부가 검증되고, 로그인 이후 세션에서는 인증여부를 판단하기 위한 식별정보로 사용된다.

접근토큰 요청메시지는 ARCTRRequestMessage의 orgCode 필드를 사용하며, 기관코드값을 가져야 한다.

6.3.4.2 접근토큰 응답 (OP0002)

접근토큰 응답은 접근토큰 요청의 처리내역에 대한 응답메시지를 나타낸다.

ARCTRResponseMessage의 arctrRespAccessToken는 접근요청에 대한 서버가 생성한 식별정보로 16바이트 랜덤값을 갖는다.

6.3.4.3 로그인 요청 (OP0003)

로그인 요청은 사용자 인증을 위해 수행한 절차로, '인증서 기반' 방식과 'ID/Password' 방식 모두를 지원하여야 한다. 이 규격에서는 '인증서 기반'

로그인 절차를 필수항목으로 사용하여야 한다.

로그인 요청을 위해서는 수신모듈에 사전에 송신모듈을 등록하는 절차를 거쳐야 한다. 이 규격에서는 사전등록절차는 기술하지 않는다. 다만, 수신모듈에서는 송신모듈의 ID, 패스워드, 그리고 인증서의 DN정보를 별도 저장하여 관리하여야 한다.

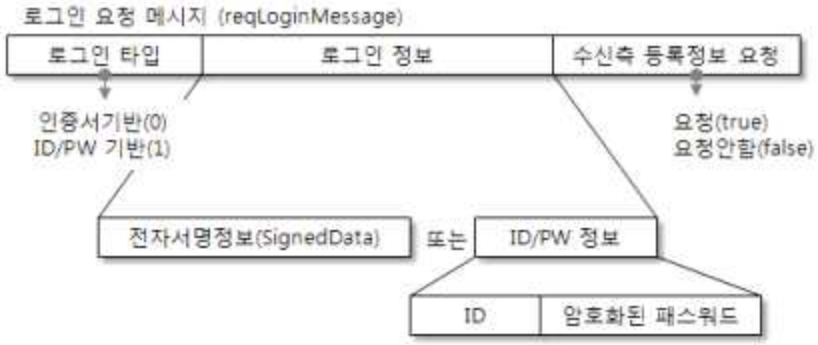

그림 25 - 로그인 요청메시지 구조

```
reqLoginMessage ::= SEQUENCE {
        loginType               arctrLoginType,         -- 로그인 방식
        loginData               arctrLoginInfo,         -- 로그인 요청정보
        reqRecvReg      [0]     BOOLEAN OPTIONAL -- 수신모듈 등록정보 요청
}
```

- loginType은 인증서 기반 또는 ID/패스워드 방식에 대한 구분자를 나타낸다. 해당 방식에 대한 로그인 생성정보는 loginData에 기술되어야 한다.
- loginData는 인증서 기반의 로그인 정보 또는 ID/Password 기반의 로그인 정보 중 하나를 가져야 한다.
- reqRecvReg는 수신모듈의 등록정보를 요청할지 여부를 나타내는 것으로 true이면 요청을, false이면 요청하지 않음을 나타낸다. 수신모듈은 해당 필드가 true로 설정되어 있으면 로그인 응답메시지는 ID, 패드워드, 그리고 인증서 DN정보를 반드시 포함하여 응답하여야 한다.

```
arctrLoginType ::= ENUMERATED {
        certificateLogin        (0),    --인증서 기반 로그인
        idPasswordLogin         (1)     --ID/Password 기반 로그인
```

```
}
arctrLoginInfo ::= CHOICE {
        signedLoginData     ContentInfo,   -- PKCS#7의 ContentInfo(SignedData)
        idPassword          idpwDataInfo -- ID and password 정보
}
```

- signedLoginData는 '접근토큰 응답메시지' 내의 접근토큰(ARCTRResponseMessage. arctrRespAccessToken)에 대한 전자서명값을 가진다. 전자서명값은 CMS의 SignedData를 이용하며, SignedData는 다시 ContentInfo로 표현되어야 한다. SignedData는 접근토큰, 서명값, 그리고 서명자 인증서 등의 정보를 포함하고 있으며, 수신모듈은 전자서명값 및 인증서의 기본검증, 경로검증, 상태검증을 포함한 유효성을 반드시 검증하여야 한다. (참고문헌 [4], [15])
- idPassword는 송신모듈의 ID와 패스워드 정보, 그리고 접근토큰을 가져야 한다.

```
ContentInfo ::= SEQUENCE {
        contentType    ContentType,
        content        [0 EXPLICIT ANY DEFINED BY contentType OPTIONAL
}
SignedData ::= SEQUENCE {
        version                 Version,
        digestAlgorithms        DigestAlgorithmIdentifiers,
        contentInfo             ContentInfo,
        certificates        [0] IMPLICIT ExtendedCertificatesAndCertificates OPTIONAL,
        crls                [1] IMPLICIT CertificateRevocationLists OPTIONAL,
        signerInfos             SignerInfos
}
```

- contentInfo는 서명할 원본정보로 '접근토큰'을 가져야 한다.
- SignedData는 서명자의 인증서를 반드시 포함하여야 한다.

```
pkcs-7 OBJECT IDENTIFIER ::= { iso(1) member-body(2) US(840)
rsadsi(113549) pkcs(1) 7 }
signedData OBJECT IDENTIFIER ::= { pkcs-7 2 }
```

```
idpwDataInfo ::= SEQUENCE {
        id              OCTET STRING,     -- ID String
        password        OCTET STRING      -- SHA1(password)
        accessToken     OCTET STRING      -- 접근토큰
}
```

- id는 수신모듈에 기 등록된 ID를 나타낸다.
- password는 수신모듈에 기 등록된 패스워드를 나타낸다. 패스워드는 SHA1 해쉬알고리즘에 의해 생성된 해쉬값으로 바이너리 값이 기술된다.
- accessToken는 '접근토큰 응답메시지'내의 arctrRespAccessToken 값이 기술된다.
- 수신모듈은 반드시 등록된 ID/패스워드 그리고 접근토큰 정보와 수신한 정보를 비교 검증하여야 한다.

접근토큰(accessToken)은 추가적인 로그인 과정 없이 세션 생성 시 사용되므로 송·수신모듈은 하나의 전송목록파일 및 전송목록파일 내 전자기록물파일들이 전송 완료되는 시점까지 유지하여야 한다. 접근토큰의 유지기간은 전송목록파일 단위로 새로운 전송목록파일을 처리하기 위해서는 새로운 접근토큰이 생성되어야 한다.

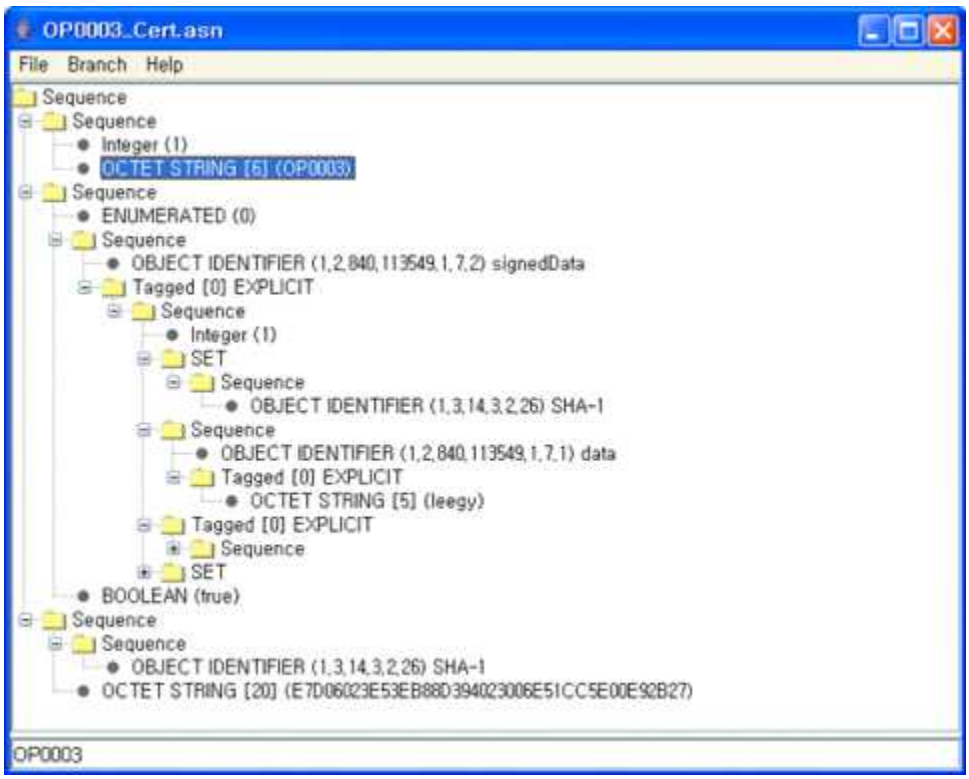

그림 26 - 예시 : 로그인 요청메시지(인증서 기반)

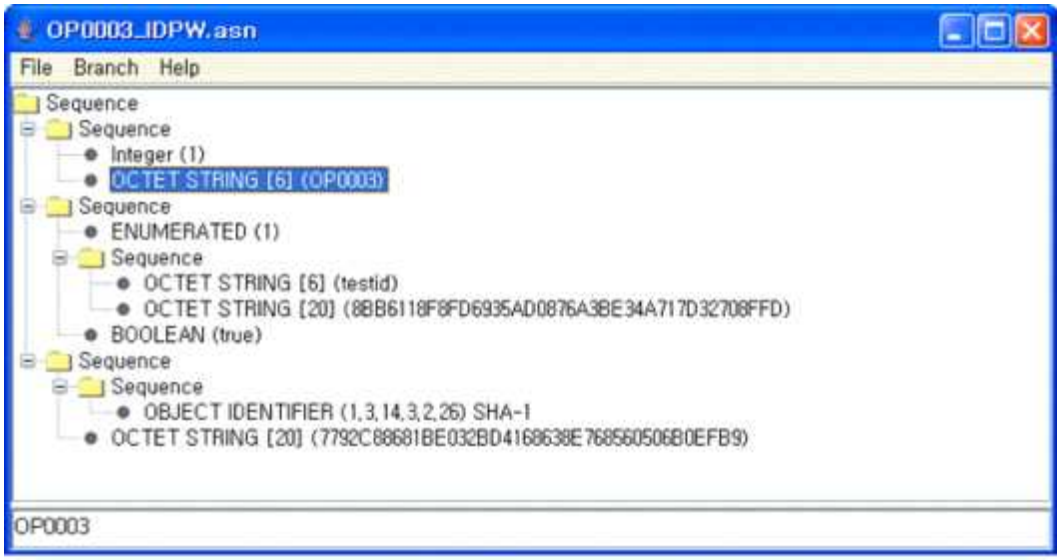

그림 27 - 예시 : 로그인 요청메시지(ID/PASSWORD 기반)

6.3.4.4 로그인 응답 (OP0004)

로그인 응답은 로그인 요청의 검증 및 처리내역에 대한 응답메시지를 나타낸다.

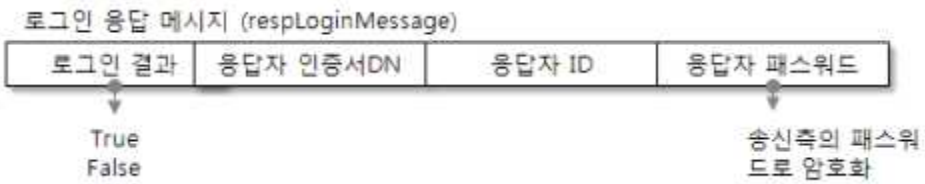

그림 28 - 로그인 응답메시지 구조

```
respLoginMessage ::= SEQUENCE {
        loginResult             BOOLEAN,                    -- true
        respCertDN        [0]   OCTET STRINGOPTIONAL,       -- 인증서 DN
        respReceiverID    [1]   OCTET STRING OPTIONAL,      -- ID
        respReceiverPW    [2]   OCTET STRING OPTIONAL       -- 암호화된 패스워드
}
```

- loginResult은 로그인 허용여부를 나타내는 값으로, 항상 true값을 가져야 한다. 만일 로그인이 허용되지 않으면 ARCTRResponseMessage는 ErrorMessage를 가지며, 오류코드 및 오류메지를 기술하여야 한다.
- respCertDN는 응답메시지 생성자의 인증서DN을 나타낸다. DN은 문자

열로 표현되고 대소문자 구분은 없다. 로그인 요청메시지의 reqLoginMessage. reqRecvReg가 true이면 이 필드는 반드시 설정되어야 한다.

- respReceiverID는 응답메시지 생성자의 ID를 나타낸다. ID는 문자열로 표현되고 대소문자를 구분해야 한다. 로그인 요청메시지의 reqLogin Message. reqRecvReg가 true이면 이 필드는 반드시 설정되어야 한다.
- respReceiverPW는 응답메시지 생성자의 패스워드 정보를 나타낸다. 로그인 요청메시지의 reqLoginMessage. reqRecvReg가 true이면 이 필드는 반드시 설정되어야 한다. 패스워드 정보는 등록된 요청자의 비밀번호를 이용하여 대칭키 알고리즘으로 암호화한 바이너리 값을 가져야 한다. 대칭키 알고리즘은 SEED_CDC 알고리즘을 사용하고, 키 유도함수는 PKCS#5의 PBKDF(버전 1.5)을 사용하여 key(키)와 iv(초기벡터)를 유도한다. PBKDF에서 사용되는 해쉬알고리즘은 SHA1 해쉬알고리즘을 사용한다. 이때 사용되는 salt와 iteration count는 고정된 값을 사용하며, 이는 별도의 절차로 공표한다. (세부 절차는 참고문헌 [16] 참조)
- 로그인 응답메시지 수신자는 수신한 respCertDN, respReceiverID 및 복호화된 패스워드 정보를 저장·관리하여야 하고, 향후 역으로 로그인 시 사용되어야 한다.

그림 29 - 예시 : 로그인 응답메시지

6.3.4.5 로그아웃 요청 (OP0005)

로그아웃 요청은 송·수신 모듈 간 로그아웃을 요청하는 메시지이다.

로그아웃 요청메시지는 ARCTRRequestMessage의 orgCode필드를 사용하며, 기관코드값을 가져야 한다.

6.3.4.6 로그아웃 응답 (OP0006)

로그아웃 응답은 로그아웃 요청메시지에 대한 응답메시지를 나타낸다.

로그아웃 응답메시지는 ARCTRRequestMessage의 orgCode필드를 사용하며, 요청메시지와 동일한 기관코드값을 가져야 한다.

로그아웃 절차 이후에는 '접근토큰 요청' 및 '접근토큰 응답'에서 교환한 '접근토큰'은 더 이상 사용되지 않는다.

6.3.4.7 전송통지 요청 (OP0011)

전송통지 요청은 파일전송을 위해 사전 검사를 위한 요청메시지를 나타낸다. 이 요청메시지는 전송목록파일 및 전자기록물파일 전송을 위한 사전 준비단계에 수행되어야 한다. 또한 전송목록파일에 나열된 전자기록물파일들을 모두 전송했다는 통보메시지로도 사용되어야 한다.

그림 30 - 전송통지 요청메시지 구조

```
reqNotiMessage ::= SEQUENCE {
        accessToken             OCTET STRING,       -- 접근토큰
        fileType                arctrFileType,
```

```
    fileName            OCTET STRING,
    fileSize            INTEGER,
    listFileName        OCTET STRING,
    orgCode             OCTET STRING,
    sendDir         [0] OCTET STRING    OPTIONAL,
    relPathInfo     [1] OCTET STRING    OPTIONAL,
    arcFileCount    [2] INTEGER         OPTIONAL
}
```

- accessToken은 ARCTRResponseMessage의 arctrRespAccessToken값을 가져야 한다.
- fileType은 전송할 파일의 종류를 나타낸다.
- fileName은 전송할 파일명으로, fileType에 따라 각기 다른 정보를 기입하여야 한다. fileType = 0 : '전송목록파일명.xml'을 기술해야 한다. fileType = 1 : '전송목록파일'의 'rel_path_info'에 기술된 정보 중 파일명을 기술해야 한다. fileType = 2 : '전송목록파일명.end'를 기술해야 한다.
- fileSize는 전송할 파일의 크기정보로, '전송목록파일'의 'file_size' 정보를 사용할 수 있다.
- listFileName는 fileName과 연관된 전송목록파일명을 나타낸다. fileType이 '0'이면 listFileName은 fileName과 동일한 값을 가져야 한다.
- orgCode는 기관코드값으로, '전송목록파일'의 'org_code' 정보로 설정하여야 한다.
- sendDir는 전송디렉토리 정보로, fileType이 '1'인 경우에는 반드시 '전송목록파일'의 'send_dir' 정보로 설정하여야 한다. 그 외는 이 필드를 사용하지 않는다.
- relPathInfo는 파일명 또는 상대경로를 포함한 파일명 정보로, fileType이 '1'인 경우에는 반드시 '전송목록파일'의 'rel_path_info' 정보로 설정하여야 한다.

  fileType이 '0'이거나 '2'일 경우에는 전송목록파일이 sendlist 디렉토리 내에 하위 디렉토리 구조를 가지는 경우에 한해서는 이 필드를 사용하여야 하고, 그렇지 않는 경우에는 사용하지 않는다.
- arcFileCount는 전송목록파일에 기술된 전자기록물일들의 개수로, fileType이 '0'인 경우에는 반드시 개수를 설정하여야 한다. 그 외는 이 필드를 사용하지 않는다.

```
arctrFileType ::= ENUMERATED {
        tbSentListFile  (0),        --전송목록파일 전송
        tbSentArcFile   (1),        --전자기록물파일 전송
        isSentEndFile   (2)         --전자기록물파일 전송완료
}
```

- tbSentListFile는 전송할 파일이 '전송목록파일'임을 의미한다. 송신모듈은 이후 '파일전송 요청메시지'를 이용하여 '전송목록파일'을 전송하여야 한다. 수신모듈은 '전송통지 요청'에 대한 응답을 수행한 후 '전송목록파일'을 수신 대기하여야 한다.
- tbSentArcFile은 전송할 파일이 '전자기록물파일'임을 의미한다. 송신모듈은 이후 '파일전송 요청메시지'를 이용하여 '전자기록물파일'을 전송하여야 한다. 수신모듈은 '전송통지 요청'에 대한 응답을 수행한 후 '전자기록물파일'을 수신 대기하여야 한다.
- isSentEndFile은 해당 전송목록파일에 대한 전자기록물파일 전송이 완료되었음을 의미한다. 수신모듈은 수신한 '전송목록파일'과 '전자기록물파일'의 파일 일치성 검사를 수행한 후, '전송통지 요청'에 대한 응답을 수행하여야 한다. 또한 수신모듈은 전송통지 응답메시지 전송 후, 파일 일치성 검사 성공 시 해당 전송목록파일에 대해 시점확인 토큰을 생성하여야 한다.

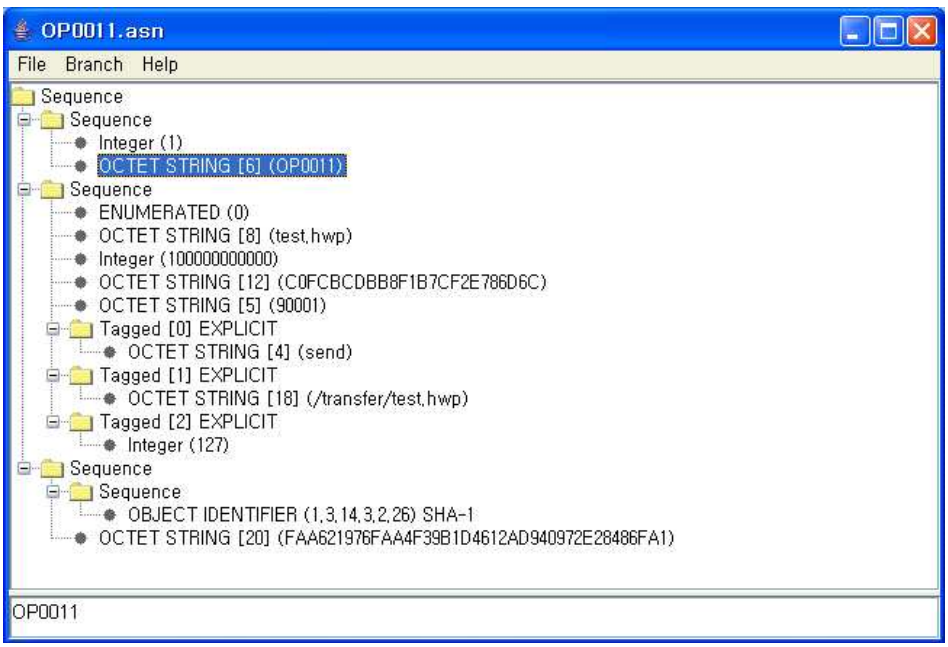

그림 31 - 예시 : 전송통지 요청메시지

6.3.4.8 전송통지 응답 (OP0012)

전송통지 응답은 '전송통지 요청'에 대한 응답메시지를 나타낸다. 수신모듈에서는 수신한 '전송통지 요청메시지'에 대해 처리 중 오류가 발생하면 오류메시지를 전달하여야 하고, 오류메시지를 수신한 송신모듈은 해당 전송목록파일 또는 전자기록물파일에 대하여 전송실패로 처리하여야 한다.

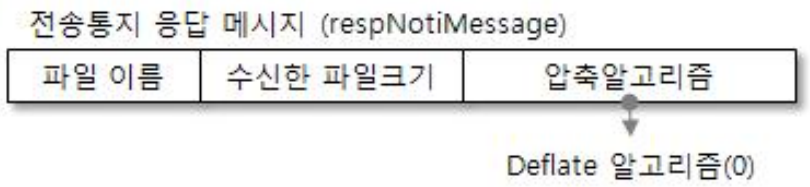

그림 32 - 전송통지 응답메시지 구조

```
respNotiMessage ::= SEQUENCE {
        fileName              OCTET STRING,
        currentFileSize       INTEGER              --이미 수신한 파일크기
        compressAlg      [0]  compressionAlgInfo OPTIONAL
}
```

- fileName은 '전송통지 요청'메시지에 기술된 파일명으로 설정하여야 한다.
- currentFileSize는 '전송통지 요청' 메시지에 기술된 경로의 파일에 대하여, 이미 수신완료한 파일의 크기를 나타낸다.

  만일 해당파일이 존재하지 않으면 currentFileSize는 0으로 설정하여야 한다.
  만일 '전송통지 요청메시지'의 fileType이 '0'이면 이미 수신완료한 파일크기와 무관하게 '0'을 설정하여야 한다. 이는 해당 전송목록파일을 새로이 재전송하기 위해서이다.
  만일 '전송통지 요청메시지'의 fileType이 '1'이면 이미 수신완료한 파일의 크기를 설정하여야 한다.
  송신모듈은 currentFileSize가 '0'이면 해당 파일을 '파일전송 요청메시지'를 통해 처음부터 전송하여야 하고, 1보다 크거나 같고 전송할 파일크기보다 작으면 해당 파일 전송 중 에러가 발생한 것으로

courentFileSize 이후의 파일블록을 '이어보내기' 한다.
단, 해당 파일이 전자기록물파일이고 전송목록파일 내 is_resend값이 '1'인 경우, 송신모듈은 전송통지 응답메시지의 'currentFileSize' 값과 무관하게 해당 파일을 '재전송'한다.
currentFileSize가 전송통지 요청메시지 내의 fileSize보다 크면 이는 수신모듈이 잘못된 파일을 보관하고 있는 경우이므로 파일을 처음부터 전송해야 하고, 동일할 경우에는 전송완료로 판단한다. fileType이 '2'이면 해당 전송목록파일에 대한 전자기록물파일 전송완료를 나타내는 것으로 '0'이 설정되어야 한다.

- compressAlg은 수신모듈에서 지원하는 압축알고리즘 종류를 나타내는 값으로, 이 필드 사용 시 deflateAlg(0)로 설정하여야 한다.

```
compressionAlgInfo ::= ENUMERATED {
        deflateAlg      (0),            -기본알고리즘으로 사용함
        otherAlg        (1)
}
```

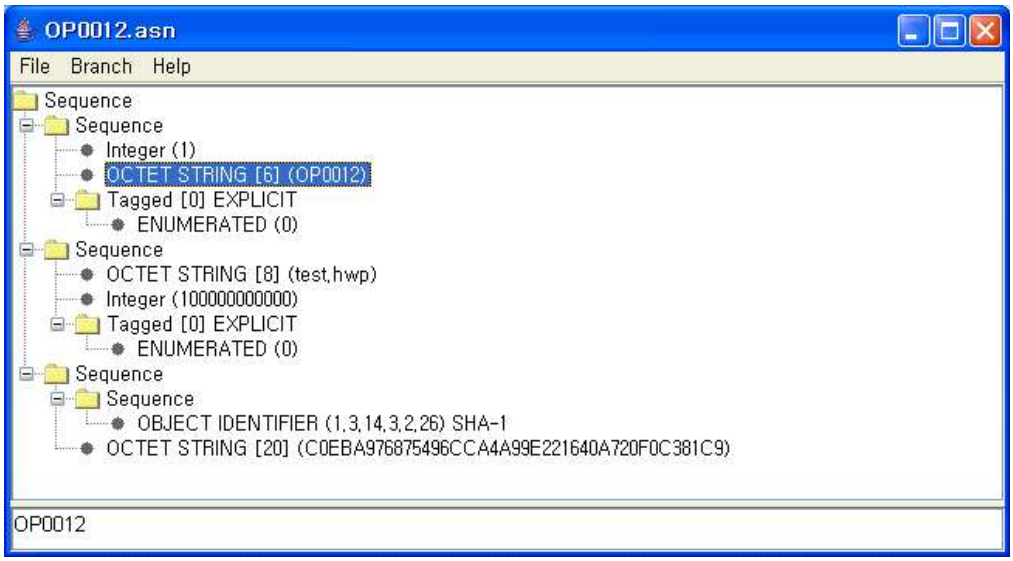

그림 33 - 예시 : 전송통지 응답메시지

6.3.4.9 파일전송 요청 (OP0013)

파일전송 요청은 파일을 블록단위로 전송하기 위한 요청메시지를 나타낸다. 이 요청메시지는 반드시 '전송통지 요청메시지' 이후에 수행되어야 하며, 2번

이상 연속적으로 사용 가능하다.

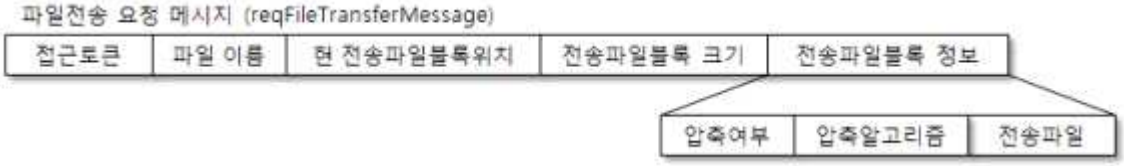

그림 34 - 파일전송 요청메시지 구조

```
reqFileTransferMessage ::= SEQUENCE {
        accessToken             OCTET STRING,      -- 접근토큰
        fileName                OCTET STRING,
        curFilePosition         INTEGER,
        curFileLength           INTEGER,
        transFileData           arctrTransDataInfo
}
```

- accessToken은 ARCTRResponseMessage의 arctrRespAccessToken값을 가져야 한다.
- fileName은 현재 전송 중인 파일명으로, 전송목록파일 전송 시 전송목록파일명이 기술되고, 전자기록물파일을 전송하는 경우에는 '전송목록파일'의 'rel_path_info'에 기술된 내용 중 파일이름이 기술되어야 한다.
- curFilePosition은 현재 전송 중인 파일블록의 시작위치(파일포인터)를 나타낸다. 수신모듈은 수신한 transFileData를 지정된 파일포인터의 절대위치에 쓸 수 있어야 한다.
- curFileLength는 현재 전송 중인 파일블록의 크기를 나타낸다. 파일블록의 크기는 transFileData의 파일정보의 크기로, 압축이 적용되기 전 원본파일블록의 크기로 설정해야 한다. 수신모듈은 수신한 파일블록을 curFilePosition위치에 curFileLength 크기만큼 파일로 쓸 수 있어야 한다.
- transFileData는 현재 전송 중인 파일블록의 정보를 나타낸다. 파일블록정보는 압축되어 전송될 수 있다.

```
arctrTransDataInfo ::= SEQUENCE {
        isCompressed            BOOLEAN,
        compressAlg       [0]   compressionAlgInfo   OPTIONAL,
```

transData OCTET STRING

}

- isCompressed는 해당 파일블록이 압축되었는지의 여부를 나타낸다. isCompressed가 true이면 압축되었음을 나타낸다. 만일 현재 전송할 파일이 전송목록파일일 때는 반드시 압축되어야 하고, 전자기록물파일일 때에는 전송목록파일 내의 'tb_compressed'가 '1'이면 압축을 수행해야 하고, 그렇지 않은 경우에는 압축을 수행하지 않아야 한다.
- compressAlg는 해당 파일블록의 압축알고리즘을 나타낸다. 'isCompressed' 필드가 'true'이면 deflateAlg(0)이 설정되어야 하고, 'false'이면 이 필드는 사용하지 않는다.
- transData는 전송할 파일블록정보를 나타낸다. 이 필드는 압축 또는 원본형태의 정보를 가져야 한다.

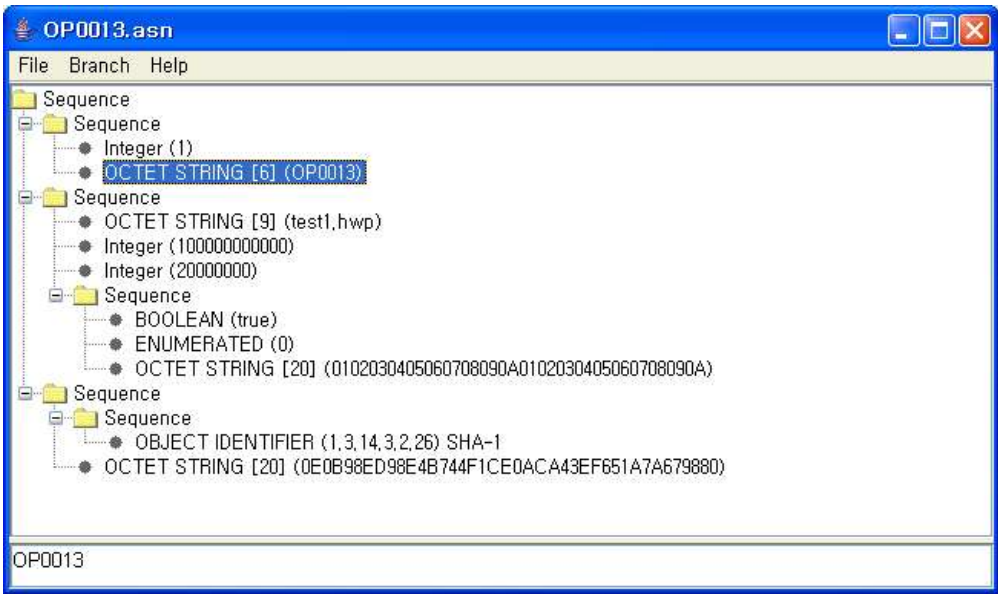

그림 35 - 예시 : 파일전송 요청메시지

6.3.4.10 파일전송 응답 (OP0014)

파일전송 응답은 '파일전송 요청'에 대한 응답메시지를 나타낸다. 수신모듈에서는 수신한 '파일전송 요청메시지'에 대해 처리 중 오류가 발생하면 오류메시지를 전달하여야 하고, 오류메시지를 수신한 송신모듈은 해당 전자기록물파일에 대해 전송실패로 처리하여야 한다.

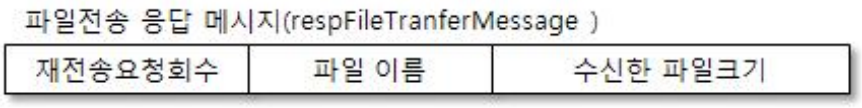

그림 36 - 파일전송 응답메시지 구조

```
respFileTranferMessage ::= SEQUENCE {
        reSendReqCount      INTEGER,
        fileName            OCTET STRING,
        totalFileSize       INTEGER      --현재까지 수신완료한 파일크기
}
```

- reSendReqCount는 reqFileTransferMessage를 통해 전달된 해당 파일블록에 대한 수신모듈의 재전송 요청횟수를 나타내며, 재전송 요청 없이 요청문의 정상처리에 대한 응답메시지는 '0'을 가져야 한다. 수신모듈은 reqFileTransferMessage 메시지를 통해 전달된 파일블록 처리 중 오류가 발생하면, 해당 블록을 재전송 요청하여야 한다. 요청메시지 처리오류로 인해 재전송 요청 시는 1부터 시작하여 해당블록의 재전송 요청 시마다 1씩 증가하고, 재전송된 파일블록을 정상 처리한 경우에는 오류횟수를 0으로 초기화한다. 재전송 요청횟수는 '6.1.4. 파일전송 절차'에서 정의한 c_5 값을 가지고, c_5 동안 해당 파일블록을 처리하지 못하면 오류메시지를 응답하여야 한다. 송신모듈은 reSendReqCount가 1 이상의 값을 가지면 해당 파일블록을 재전송하여야 한다.
- fileName은 현재 전송 중인 파일명으로, '파일전송 요청'의 'fileName'에 기술된 파일명을 가져야 한다.
- totalFileSize은 전송 중인 파일의 현재까지 수신 완료한 총 크기를 나타낸다. 송신모듈은 수신 완료된 이후의 파일블록을 전송하여야 한다. totalFileSize와 reqNotiMessage.fileSize가 일치하면 해당 파일전송이 완료되었음을 의미한다. 만일 totalFileSize가 reqNotiMessage.fileSize보다 크면 해당 파일블록을 저장하지 않고, '파일전송 응답메시지'에서 오류내역을 송신모듈에 전달 한 후, 해당 파일에 대해 전송을 중단한다.

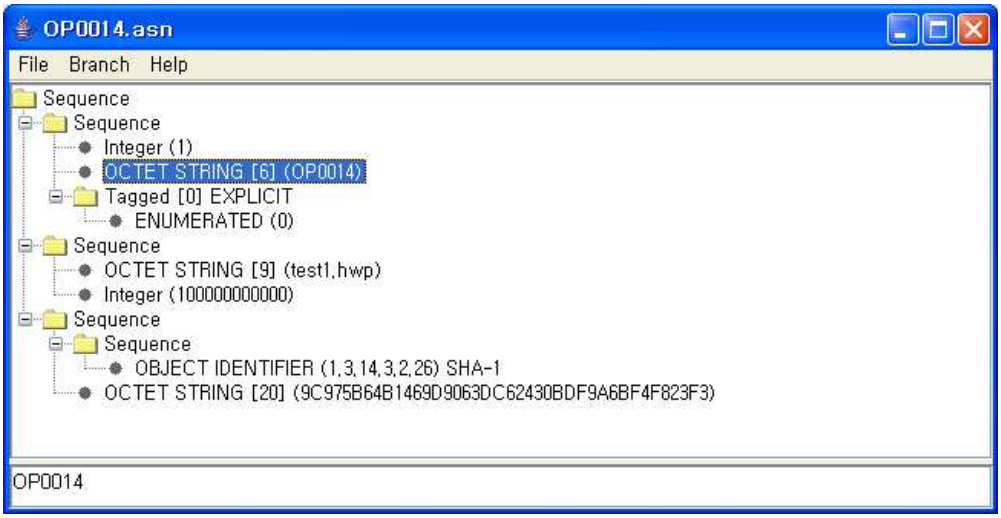

그림 37 - 예시 : 파일전송 응답메시지(정상)

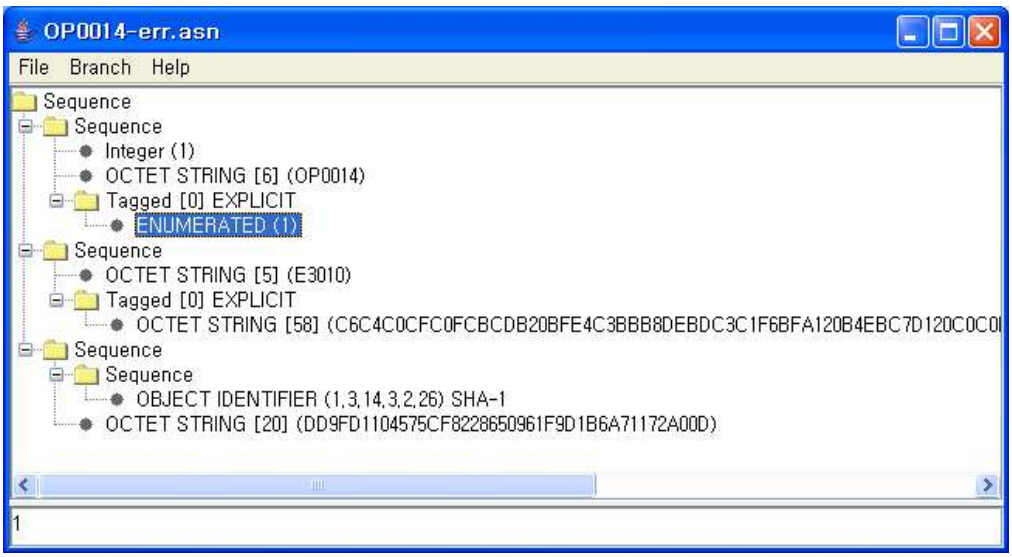

그림 38 - 예시 : 파일전송 응답메시지(오류)

6.3.4.11 연결해제 요청 (OP0015)

연결해제 요청은 송·수신 모듈 간 연결된 tcp socket 연결 해제를 요청하는 메시지이다.

연결해제 요청메시지는 ARCTRRequestMessage의 orgCode필드를 사용하며, 기관코드값을 가져야 한다.

6.3.4.12 연결해제 응답 (OP0016)

연결해제 응답은 연결해제 요청메시지에 대한 응답메시지를 나타낸다.

연결해제 응답메시지는 ARCTRRequestMessage의 orgCode필드를 사용하며, 요청메시지와 동일한 기관코드값을 가져야 한다.

연결해제 요청을 수신한 수신모듈은 현제 세션에서 사용 중인 자원반납 등과 같은 일련의 작업을 수행한 후, 연결해제 응답메시지를 전달하여야 한다.

6.4 로그포맷

6.4.1 모니터링을 위한 로그포맷

전송소프트웨어는 송신모듈 및 수신모듈 모두 전자기록물 전송 결과와 시스템의 정상작동여부를 확인할 수 있는 로그파일을 생성하여 관리하여야 한다. 이 로그파일은 시스템 모니터링 정보로 활용될 수 있다.

전송소프트웨어는 기관코드, 전송목록파일명, 전자기록물 파일개수, 전송중인 전자기록물 파일명, 전송시작시간, 전송완료시간, 처리 소요시간, 전송률의 내역을 모니터링 할 수 있는 기능을 제공하여야 한다.

(a) 로그파일 생성규칙

- {전송소프트웨어 설치경로}/log/{로그파일명은 제품에 의존}
- 로그파일명은 '6.4.2 오류내역을 위한 로그포맷'에서 정의한 파일명과 구분

(b) 로그정보

- 로그정보 생성일자
- 서비스구분 (전자기록물전송, 시스템검사)
- 기관코드값
- 요청자 IP주소
- 전송목록파일명
- 전송목록파일 내에 기술된 전자기록물파일 개수 (전송목록파일일 경우 기술)
- 파일명

- 서비스 성공여부
- 서비스요청 시작시간
- 서비스처리 완료시간
- 처리 소요시간

(c) 로그파일 사용 규칙

- 모든 제품은 아래와 같은 형식으로 로그를 기록하여야 한다.
- 로그항목은 순서를 준수하여야 한다.
- 하나의 로그정보는 '#' 문자로 시작하고, '#' 문자로 끝나야 한다.
- 하나의 로그정보는 한 줄로만 구성되어야 한다.
- 로그정보의 각 값의 구분자는 '#' 문자를 사용하여야 한다.

표 9 - 모니터링 로그파일 구성요소

항목명	최대길이	설명
성공/실패 여부	1 (고정)	• 성공 : 'S', 실패: 'F'
서비스 구분	1 (고정)	• 전자기록물전송 : 'T', 시스템검사 : 'C'
로그 생성시간	23 (고정)	• 현 로그파일 생성시간을 기록 • 형식: ''yyyy-MM-dd HH:mm:ss:SSS'' • 예제: 2010-08-23 07:01:41:596
기관코드값	10 (가변)	• 요청문의 기관코드로, 정보 획득이 불가하면 ''(공백문자)를 기록 • 형식: 문자열 • 예제: 190000
IP 주소	15 (가변)	• 서비스 요청자의 IP주소로, 시스템 검사 시는 ''(공백문자)를 기록 • 형식: xxxx.xxxx.xxxx.xxx • 예제: 123.456.789.123
전송목록파일명	가변	• 아래 '파일명'이 속한 전송목록파일의 파일명으로, 정보 획득이 불가하면 ''(공백문자)를 기록 • 형식: 파일명(.확장자) • 예제: 전송목록파일명.xml
전자기록물파일 개수	5(가변)	• 해당 파일이 전송목록파일일 경우, 전송목록파일 내에 기술한 전자기록물파일 개수. 이외의 파일에서는 ''(공백문자)를 기록 • 형식: 숫자형 문자열 • 예제: 120
파일명	가변	• 전자기록물파일명으로, 정보 획득이 불가하면 ''(공백문자)를 기록

항목명	최대길이	설명
		• 형식: 파일명(.확장자) • 예제: 테스트기록물.doc
서비스 요청시간	23 (고정)	• 해당 작업이 요청된 시간을 기록 • 형식: yyyy-MM-dd HH:mm:ss:SSS • 예제: 2010-08-23 06:56:41:594
서비스처리 완료시간	23 (고정)	• 해당 작업이 완료된 시간을 기록 • 형식: yyyy-MM-dd HH:mm:ss:SSS • 예제: 2010-08-23 07:01:41:594
소요시간	16 (가변)	• 해당 파일에 대한 전송소요시간 또는 시스템 검사 소요시간 • 형식: millisec기준 소요시간 기술 • 예제: 12000

(d) 로그파일 예제

#S#T#2010-08-23 16:05:44:494#190000#123.456.789.123#테스트기록물.doc#2010-08-23 06:56:41:594#2010-08-23 07:01:41:594#12000# [엔터]

#S#C#2010-08-23 16:05:44:494##127.0.0.1##2010-08-23 16:05:44:494#2010-08-23 16:05:44:494#1# [엔터]

#F#T#2010-08-23 16:05:44:494#190000#123.456.789.123#테스트기록물.doc#2010-08-23 06:56:41:594#2010-08-23 07:01:41:594#12000# [엔터]

6.4.2 오류내역을 위한 로그포맷

전송소프트웨어는 전자기록물 전송 중 발생된 오류내역을 확인할 수 있는 로그파일을 생성하여 관리하여야 한다. 이 규격에서는 '오류코드' 및 '오류메시지'를 정의하고, 해당 오류메시지에 대한 '오류세부내역'은 제품별로 정의하여 사용할 수 있다.

본 로그파일은 업무시스템에서 참조할 수 있다.

(a) 로그파일 생성규칙

- {전송소프트웨어 설치경로}/log/{로그파일명은 제품에 의존}
- 로그파일명은 '6.4.1 모니터링을 위한 로그포맷'에 정의된 파일명과 구분

(b) 로그정보

- 로그정보 생성일자

- 서비스 성공여부
- 서비스구분 (전송목록파일 검사, 전자기록물 전송)
- 기관코드값
- 전송목록파일명
- 파일명
- 오류코드값
- 오류메시지
- 오류세부내역

(c) 로그파일 사용 규칙

- 모든 제품은 아래와 같은 형식으로 로그를 기록하여야 한다.
- 로그항목은 순서를 준수하여야 한다.
- 하나의 로그파일은 헤더와 본문으로 구성되고, 헤더는 '로그정보 생성시간' ~ '파일명 전체경로'로 구성되고 본문은 '오류세부내역'으로 구성되어야 한다.
- 하나의 로그정보는 '#' 문자로 시작하고, '#' 문자로 끝나야 한다.
- 하나의 로그정보는 여러 라인으로 구성될 수 있어야 한다.
- 로그정보의 각 값의 구분자는 '#' 문자를 사용하여야 한다.

표 10 - 오류내역 로그파일 구성요소

항목명	최대길이	설명
성공/실패 여부	1 (고정)	• 실패: 'F'
서비스 구분	1 (고정)	• 전자기록물 전송 : 'T', 전송목록파일 검사 : 'V'
로그 생성시간	23 (고정)	• 현 로그파일 생성시간을 기록 • 형식: ''yyyy-MM-dd HH:mm:ss:SSS'' • 예제: 2010-08-23 07:01:41:596
기관코드값	10 (가변)	• 요청문의 기관코드로, 정보 획득이 불가하면 '' (공백문자)를 기록 • 형식: 문자열 • 예제: 190000
전송목록파일명	가변	• 아래 '파일명'이 속한 전송목록파일의 파일명으로, 정보 획득이 불가하면 ''(공백문자)를 기록 • 형식: 파일명(.확장자) • 예제: 전송목록파일명.xml
파일명	가변	• 전송목록파일 또는 전자기록물파일의 파일명으로, 파일명을 포함한 절대경로로 기술 • 형식: 파일명을 포함한 절대경로

항목명	최대길이	설명
		• 예제: /home/standardMD/sendlist/전송목록명.xml
오류코드값	5	• 업무시스템 연계 오류코드값 • 형식: 5자리 문자열 { 'E' + 4자리 숫자 } • 예제: E0101
오류메시지	가변	• 정의된 오류메시지를 기술 • 형식: 문자열 • 예제: 지정된 경로에 해당파일이 존재하지 않습니다.
오류세부내역	가변	• '오류메시지'의 오류발생 원인에 대한 세부내역 기술 • 형식: 문자열 • 예제: XML내에 peer_ip가 설정되어 있지 않습니다.

(d) 로그파일 예제

#F#T#2010-08-23 16:05:44:494#190000#test.xml#/home/190000/send/transfer/test.hwp#E0101# 지정된 경로에 해당파일이 존재하지 않습니다.#지정된 경로에 해당파일이 존재하지 않습니다.# [엔터]

#F#V#2010-08-23 16:05:44:494#190000#test.xml#/home/sendlist/전송목록.xml#E0102#전송목록파일의 XML 구성이 잘못되었습니다.#XML내에 peer_ip가 설정되어 있지 않습니다.# [엔터]

(e) 로그파일 정의

표 11 - 오류코드 분류

오류코드 분류	설 명
E	[1바이트] 에러코드 명기
상위 2자리 숫자	오류코드 그룹 '01' : 전송목록파일 처리 '10' : 로그인관련 요청메시지 처리 '11' : 로그인관련 응답메시지 처리 '12' : 전송통지 요청메시지 처리 '13' : 전송통지 응답메시지 처리 '14' : 파일전송 요청메시지 처리 '15' : 파일전송 응답메시지 처리 '20' : 연계시스템 연동 처리 '30' : 전송소프트웨어 내부처리
하위 2자리 숫자	해당 오류코드그룹에 대한 일련번호

표 12 - 오류코드

오류코드	오류 설명

오류코드	오류 설명
E0000	정상 처리되었습니다.
E0101	지정된 경로에 해당파일이 존재하지 않습니다.
E0102	전송목록파일의 XML 구성이 잘못되었습니다.
E0103	지정된 경로 파일에 접근할 수 없습니다. 파일의 권한을 검사하십시오.
E0104	디렉토리 구조가 잘못 구성되었습니다.
E0105	sendlist 경로가 잘못 지정되어 있습니다.
E0106	전자기록물파일의 크기를 설정할 수 없습니다.
E0107	전송목록파일 검증에 실패했습니다.
E1001	로그인 요청메시지의 구문이 잘못 구성되어 있습니다.
E1002	로그인 타입과 로그인 정보가 일치하지 않습니다.
E1003	인증서 또는 개인키 파일이 해당 경로에 존재하지 않습니다.
E1004	로그인 요청메시지의 암호화 시 오류가 발생했습니다.
E1005	개인키 비밀번호가 잘못되었습니다.
E1006	전자서명 값을 생성할 수 없습니다.
E1007	전자서명 값 형식이 잘못 구성되었습니다.
E1008	전자서명 값 검증에 실패했습니다.
E1009	서버인증서 검증에 실패했습니다.
E1010	등록된 사용자가 아닙니다. 등록업무를 먼저 수행하세요.
E1011	로그인 요청메시지 구성 중 오류가 발생했습니다.
E1101	로그인 응답메시지의 구문이 잘못 구성되어 있습니다.
E1102	로그인 요청메시지에 대한 응답메시지가 일치하지 않습니다.
E1103	수신자 등록정보 암호화에 실패했습니다.
E1104	수신자 등록정보 복호화에 실패했습니다.
E1105	등록정보가 응답메시지 내에 존재하지 않습니다.
E1106	로그인 응답메시지 구성 중 오류가 발생했습니다.
E1201	전송통지 요청메시지의 구문이 잘못 구성되어 있습니다.
E1202	파일타입이 잘못 설정되었습니다.
E1203	파일리스트가 일치하지 않아 파일 일치성 검사에 실패했습니

오류코드	오류 설명
	다.
E1204	수신한 파일크기가 일치하지 않아 파일 일치성 검사에 실패했습니다.
E1205	시점확인 토큰정보 생성에 실패했습니다.
E1206	전송통지 요청메시지 구성 중 오류가 발생했습니다.
E1301	전송통지 응답메시지의 구문이 잘못 구성되어 있습니다.
E1302	전송통지 응답메시지에 기입된 수신 파일크기가 원본 파일크기보다 큰 값입니다.
E1303	전송통지 요청메시지에 대한 응답메시지가 일치하지 않습니다.
E1304	전송통지 응답메시지 구성 중 오류가 발생했습니다.
E1401	파일전송 요청메시지의 구문이 잘못 구성되어 있습니다.
E1402	전송목록파일 전송에 실패했습니다.
E1403	전자기록물파일 전송에 실패했습니다.
E1404	전송한 파일크기와 수신대기중인 파일크기간에 GAP이 있습니다.
E1405	지원하지 않은 압축알고리즘입니다.
E1406	데이터 압축에 실패했습니다.
E1407	데이터 압축풀기에 실패했습니다.
E1408	파일전송 요청메시지 구성 중 오류가 발생했습니다.
E1501	파일전송 응답메시지의 구문이 잘못 구성되어 있습니다.
E1502	파일전송 요청메시지에 대한 응답메시지가 일치하지 않습니다.
E1503	수신완료한 파일크기가 전송한 파일크기보다 큰 값입니다.
E1504	파일전송 응답메시지 구성 중 오류가 발생했습니다.
E2001	시점확인시스템에 접속할 수 없습니다.
E2002	시점확인시스템에서 응답메시지를 수신할 수 없습니다.
E2003	인증기관 LDAP서버에 접속할 수 없습니다.
E2004	인증기관 LDAP서버에 유효한 폐지목록리스트가 존재하지 않습니다.
E2005	SSL/TLS 서버에 접속할 수 없습니다.
E2006	암호화 통신을 위해 사용된 TLS인증서 검증에 실패했습니다.
E3001	지원하지 않은 메시지 표현형식입니다.

오류코드	오류 설명
E3002	메시지 구성에 실패했습니다.
E3003	메시지의 버전정보가 잘못되었습니다.
E3004	지원하지 않은 메시지 종류입니다.
E3005	지원하지 않은 해쉬알고리즘입니다.
E3006	메시지 무결성정보 검증에 실패했습니다.
E3007	[통신오류] 수신서버에 접속할 수 없습니다. 접속할 서버정보나 방화벽을 확인하십시오.
E3008	[통신오류] 현재의 세션이 유효하지 않습니다. 세션을 종료한 후 다시 시도하십시오.

6.5 SSL/TLS 연계

본 표준에서는 연계를 위한 기본내역만 기술하며, SSL/TLS 규격은 참고문헌 [2]의 기 제정 규격을 준용하여 사용한다.

참고문헌

[1] IETF, *RFC1951, DEFLATE Compressed Data Format Specification version 1.3,* 1996년 5월

[2] IETF, *RFC2246, The Transport Layer Security (TLS) Protocol*, 1999년 1월

[3] IETF, *RFC3161, Internet X.509 PublicKey Infrastructure Time-Stamp Protocol (TSP)*, 2001년 8월

[4] IETF, *RFC3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, 2002년 4월

[5] ISO/IEC and ITU-T, *X.680, Abstract Syntax Notation One*, 1995년

[6] NIST, *FIPS PUB 180-1, SHA-1, National Institute of Standards and Technology*, 1994년

[7] NIST, *FIPS PUB 180-3, SHA-2, National Institute of Standards and Technology*, 2008년

[8] NIST, *FIPS PUB 46-3(1999), DATA ENCRYPTION STANDARD(DES)*, 1999년

[9] RSA, *PKCS#1 v2.0, RSA Cryptography Standard*, 1998년 10월

[10] RSA, *PKCS#5(1999), Password-Based Cryptography Standard*, 1999년

[11] RSA, *PKCS#7 v1.5, RSA Cryptographic Message Syntax Standard*, 1993년 11월

[12] RSA, *PKCS#8(1993), Private-Key Information Syntax Standard*, 1993년

[13] 한국인터넷진흥원, *KCAC.TG.OID, 전자서명인증관리체계 OID 가이드라인 v1.30*, 2008년

[14] 한국인터넷진흥원, *KCAC.TS.CRLPROF, 전자서명 인증서 효력정지 및 폐지목록 프로파일 규격 v1.50*, 2009년

[15] 한국인터넷진흥원, *KCAC.TS.ENC, 암호 알고리즘 규격 v1.21*, 2009년 9월

[16] 한국정보통신기술협회(TTA), *정보통신용어사전*, 2013년 6월[2013년 6월 열람], <http://word.tta.or.kr/terms/terms.jsp>