

# 공공 웹사이트 플러그인 제거 가이드라인

2018. 11.



본 가이드라인은 “민원 처리에 관한 법률 시행령”개정 이전에 배포됨으로, 향후 신규 공공 웹사이트 구축을 하거나 기존 공공 웹사이트의 플러그인을 제거할 경우, 관련 법 개정 여부를 확인하고 제거 시점의 규정에 적합한 플러그인 대체(제거) 방안을 선택하는 것을 권장함

본 가이드라인에 포함된 웹사이트 사례는 예시일 뿐, 해당 웹사이트에 적용된 솔루션을 권장하거나 추천하는 것이 아님



# 목 차

## I 가이드라인 개요

- 1. 배경 6
- 2. 목적 및 활용 대상 6

## II 플러그인 현황 분석

- 1. 플러그인 사용 배경 8
- 2. 사용 목적별 구분 9
- 3. 기술 유형별 구분 10
- 4. 웹표준 기술(HTML5) 15

## III 플러그인 제거 방안

- 1. 개요 18
- 2. 본인확인 21
- 3. 전자서명 31
- 4. 전자결제 38
- 5. PC 및 공인인증서 보안 46
- 6. 전자문서 조회 및 보안 55
- 7. 출력물 위변조 방지 및 프린터 제어 69
- 8. 멀티미디어 및 파일처리 등 78
- 9. 기타 플러그인 및 브라우저 userAgent 84

## IV 부 록

- 1. 질의 및 응답(Q&A) 87
- 2. 표 목차 91
- 3. 그림 목차 92
- 4. 용어 설명 94
- 5. 약어 96
- 6. 참고 문헌 97

# I

## 가이드라인 개요

1. 배경
2. 목적 및 활용 대상

# I. 가이드라인 개요

## 1 배경

지난 10여 년간 공공 웹사이트에서 광범위하게 사용된 플러그인으로 인해 다음과 같은 문제가 발생

### □ 기술종속

- 특정 브라우저 기반 확장 기술의 과도한 사용은 특정 운영체제와 브라우저에 이용 환경과 개발환경이 종속되는 문제 발생

### □ 보안 취약성

- 플러그인의 자체 보안 취약점과 이용자의 관행적인 플러그인 설치 문화에 따른 잠재적 보안 위험 증가

### □ 이용자 불편

- 웹사이트 별 플러그인 중복 설치로 인한 PC 속도 저하와 설치 시 브라우저 강제 종료, 메모리 충돌로 인한 PC 종료 등의 이용자 불편 초래

최신 웹표준 기술인 HTML5.X는 플러그인이 제공했던 여러 기능을 제공하고 있어, 이를 이용하여 다수의 플러그인을 제거·대체하고, 대체할 수 없는 플러그인은 이용절차 변경이나 필요성 재검토를 통해 제거하고자 함

## 2 목적 및 활용 대상

공공 웹사이트 플러그인 제거 가이드라인은 국내 공공기관 대민용 웹사이트 운영자 및 개발자가 아래와 같은 목적을 수행하는데 참고 할 수 있도록 작성함

- ⊕ 기존 공공 웹사이트의 플러그인 기능을 웹표준 기술로 전환 시
- ⊕ 신규 공공 웹사이트에 플러그인 설치 없이 구축 시

공공 웹사이트 플러그인 제거 가이드라인 활용 대상

- ⊕ 공공 웹사이트 운영(기획) 담당자
- ⊕ 공공 웹사이트 개발 담당자

 플러그인 : 브라우저가 제공하지 않는 기능을 사용하기 위해 피시(PC)에 설치하고 브라우저와 연동하여 사용하는 별도의 소프트웨어

# II

## 플러그인 현황 분석

1. 플러그인 사용 배경
2. 사용 목적별 구분
3. 기술 유형별 구분
4. 웹표준 기술(HTML5)

## II. 플러그인 현황 분석

### 1 플러그인 사용 배경

기존 대면 방식의 업무 절차를 온라인으로 전환하면서 이용 편의성 제고와 보안 강화를 목적으로 웹표준에서 지원이 불가능한 기능을 제공하기 위해 플러그인 사용

- 온라인상의 비대면 본인확인 및 전자서명 기능을 제공하기 위한 공인인증서 관련 플러그인 사용
- 웹브라우저에서 문서열람, 다양한 그래프 표현, 동영상 재생 등 이용자 편의를 위한 플러그인 사용
- 개인정보보호, PC 보호를 위해 방화벽, 키보드보안 등 보안 플러그인 사용

이용자는 아래와 같은 서비스 흐름에 따라 플러그인 사용

〈표 1〉 대민용 웹서비스 이용 절차에 따른 플러그인 사용

서비스 FLOW	대민용 서비스 이용 기능(사이트에 따라 일부 기능 사용 안함)						
	①회원가입	②로그인	③정보열람	④서비스 신청	⑤전자결제	⑥문서열람 (조회)	⑦증명서 출력
플러그인 사용목적	본인확인  PC 및 공인인증서 보안	본인인증  PC 및 공인인증서 보안	전자문서 조회 및 보안  멀티미디어 및 파일처리 등	전자서명  파일 업/다운로드  기타 (원격제어 및 장치관리 등)	전자결제  전자서명  PC 및 공인인증서 보안	전자문서 조회 및 보안	출력물 위변조 방지 및 프린터 제어  증명서 진위확인

## 2 사용 목적별 구분

플러그인은 주로 이용자 본인확인 및 전자서명, 전자결제, PC 및 공인인증서 보안, 전자문서 조회 및 보안 등의 목적으로 사용됨

사용 목적		사용 목적별 설명	
1	본인확인	비대면 실명 확인 및 본인인증	
2	전자서명	부인방지, 시점확인, 진위확인	
3	전자결제	3.1 카드결제	PG를 통한 카드 결제
		3.2 계좌이체	은행 계좌 이체 송금
4	PC 및 공인인증서 보안	4.1 백신	PC 악성코드 탐지 보안
		4.2 개인방화벽 (IP 로그수집기)	PC방화벽, 안티바이러스, 침입탐지 및 차단, 공유폴더 접근차단
		4.3 키보드보안	키 입력 값 암호화, 키로깅 방지
		4.4 전송구간 암호화	송수신 암호화 솔루션
5	전자문서 조회 및 보안	5.1 조회화면 보호 (웹 DRM)	화면캡처방지, 메뉴제어, 마우스/키보드 제어, 클립보드제어, 소스보기 제어
		5.2 전자문서 조회, 보호	PDF 뷰어, 웹폼 서식 지원, 웹폼 뷰어 보안 PDF 뷰어 및 시점확인 지원
6	출력물 위변조 방지 프린터 제어	6.1 증명서(출력) 위변조 방지	2D바코드, 워터마크, 전자관인, 발급(증명)번호 표시
		6.2 종이문서 프린터 출력(매수) 제어	프린터 스톱 접근 방지, 프린터 제조사 지원 리스트 제어, 프린터 출력매수 제어
7	멀티미디어 및 파일 처리	7.1 멀티미디어	동영상(음악) 플레이어, 영상 커뮤니케이션
		7.2 리포팅툴 및 웹에디터	문서서식 작성, 편집 및 웹 콘텐츠 제작, 출력 위변조 방지 솔루션 연계
		7.3 그래픽 및 차트 그리드	연산된 값을 그래프로 표시하거나 엑셀과 유사한 테이블 뷰 및 연산 기능과 차트, 애니메이션 표시
		7.4 파일 업/다운로드	대용량 파일 전송, 다중 파일 업/다운로드(이어받기)
8	기타 (원격제어 및 장치 관리 등)	8.1 원격제어	PC(웹 서비스) 원격 제어
		8.2 장치관리	시스템 정보확인, 드라이버 접근, 메모리 커널 접근
		8.3 인증서 복사	인증서 스마트폰 복사 및 이용
		8.4 개인정보보호	개인정보 노출 방지 및 필터링

플러그인 기술 유형은 아래와 같이 구분할 수 있음

- 운영체제 개발사가 자사 브라우저 확장 기술을 제공하기 위한 경우(ex 액티브X)
- 브라우저 개발사가 멀티 OS에서 시스템 자원 연동을 제공하기 위한 경우(ex NPAPI, Native Client, PPAPI)
- 솔루션 개발사가 자사의 특정 기술(멀티미디어, 애니메이션, 그래픽 등)을 확산하기 위해 브라우저와 연동하는 경우(ex Flash Player, Silverlight)
- 기존 액티브X, NPAPI 플러그인을 대체하기 위한 경우(ex EXE)

### 액티브X

마이크로소프트에서 만든 COM(Component Object Model)과 OLE(Object Linking and Embedding) 컨트롤을 Internet Explorer(이하 IE)와 연동할 수 있도록 개발한 기술

10여 년간 사용한 액티브X의 문제점은 아래와 같음

- 이용자가 액티브X를 관행적으로 설치하여 바이러스와 악성코드가 함께 설치되는 보안취약점 발생
- IE 전용 기술로 특정 브라우저 사용 편향 및 웹서비스 호환성 저하
- 액티브X 설치를 위해 관리자 권한을 요구하거나 브라우저 보안 등급을 낮추는 문제
- 여러 운영기관에서 유사한 기능의 액티브X를 중복 설치함으로써 이용자 PC의 자원을 낭비하거나 기능 충돌로 운영체제가 종료되는 문제 발생

### ■ 액티브X 기술 유형

#### ☞ 액티브X Control

웹페이지에 내장되거나 연동하는 형태의 실행 가능한 프로그램으로 C/C++, 비주얼베이직, 델파이 등과 같은 다양한 언어로 개발

#### ☞ 액티브X Document

마이크로소프트의 MS워드, 엑셀등과 연동하기 위한 실행 객체

### ☞ 액티브X Scripting

자바스크립트나 J스크립트, VB스크립트 확장 기술

### ☞ 액티브X Data Object(ADO)

ASP에서 마이크로소프트 데이터베이스에 접근하기 위한 기술

### ☞ Browser Helper Object(BHO)

IE에서 지원하지 않는 기능을 지원하기 위해 플러그인 형태로 추가되는 Dll 객체 모듈

## ■ 파일 확장자

- 액티브X 확장자(\*.ocx, \*.cab, \*.dll)

## ■ 사용 영역

- 본인확인(공인인증서 설치, 수정, 삭제, 연동)
- 전자서명(공인인증서 설치, 수정, 삭제, 연동)
- 전자결제(결제창 설치, 수정, 삭제, 연동)
- 보안(백신, 개인방화벽, 키보드보안 설치)
- 조희화면 보호
- 출력문서 위변조 방지
- 출력문서 프린터 제어
- 멀티미디어 및 파일처리
- 원격제어 및 장치관리

## 실행파일(exe, dmg)

실행파일은 운영체제에서 코드화된 명령에 따라 지시된 작업을 수행하는 컴퓨터 파일(형식)로 운영체제 메모리에 상주하여 시스템 자원 호출이나 다른 애플리케이션(브라우저)과 메시지 교환 등에 사용

액티브X를 대체하는 실행파일은 멀티 OS, 멀티 브라우저 지원과 커널 모드 디바이스 드라이버(USB제어, 프린터 제어)가 필요한 경우 사용

## ■ 실행파일 기술 유형

### ☞ URI 프로토콜 핸들러

특정 응용 프로그램의 고유 지시어인 Custom URI Scheme을 통해 브라우저에서 다른 응용 애플리케이션을 호출하는 기술

### ☞ 로컬 웹서버 루프백 방식

실행파일 내 확장 기능과 웹서버를 동시에 설치하고 웹페이지와 로컬 웹서버 간 XHR이나 WebSocket을 통해 Localhost 방식으로 통신하고, 웹서버가 SSL로 보안(인증)서버와 통신하는 방법

### ☞ DLL injection 방식

윈도우에서 브라우저(IE) 실행 주소 공간 내에서 실행파일 프로세스에 DLL을 강제로 로드해서 특정 기능을 수행시키는 기술(해킹 위험성으로 사용 자제)

## ■ 파일 확장자

- 윈도우 실행파일 확장자(\*.exe, \*.msi), 맥 OS 실행파일 확장자(\*.dmg)

## ■ 사용 영역

- 본인확인(공인인증서 설치, 갱신, 삭제, 연동)
- 전자서명(공인인증서 설치, 갱신, 삭제, 연동)
- 전자결제(결제창 설치, 수정, 삭제, 연동)
- 보안(백신, 개인방화벽, 키보드보안 설치)
- 조회화면 보호
- 출력문서 위변조 방지
- 출력문서 프린터 제어
- 멀티미디어 및 파일처리
- 원격제어 및 장치관리

## 리치 인터넷 애플리케이션(Rich Internet Application; RIA)

과거 웹브라우저 기반 인터페이스의 단점인 늦은 응답 속도, 데스크톱 애플리케이션에서 지원하지 않는 기능 제공, 이용 편의성 등을 개선하기 위해 별도의 런타임 시스템을 설치해서 브라우저와 연동하는 방식

HTML5 웹표준 기술로 대체 가능하여, 향후 기술 지원 중단 예정

### ■ RIA 제품 리스트

- 어도비 Flash Player(AIR), 마이크로소프트 실버라이트, 오라클 애플릿(자바 FX), 투비소프트 엑스플랫폼, 슈프트정보통신 가우스 등

### ■ 사용 영역

- 멀티미디어(동영상)
- 애니메이션
- 웹 폼, 리포팅툴
- 웹 UI(그리드, 차트)
- 전자문서 조회

#### 💡 제품 수명 주기 참고

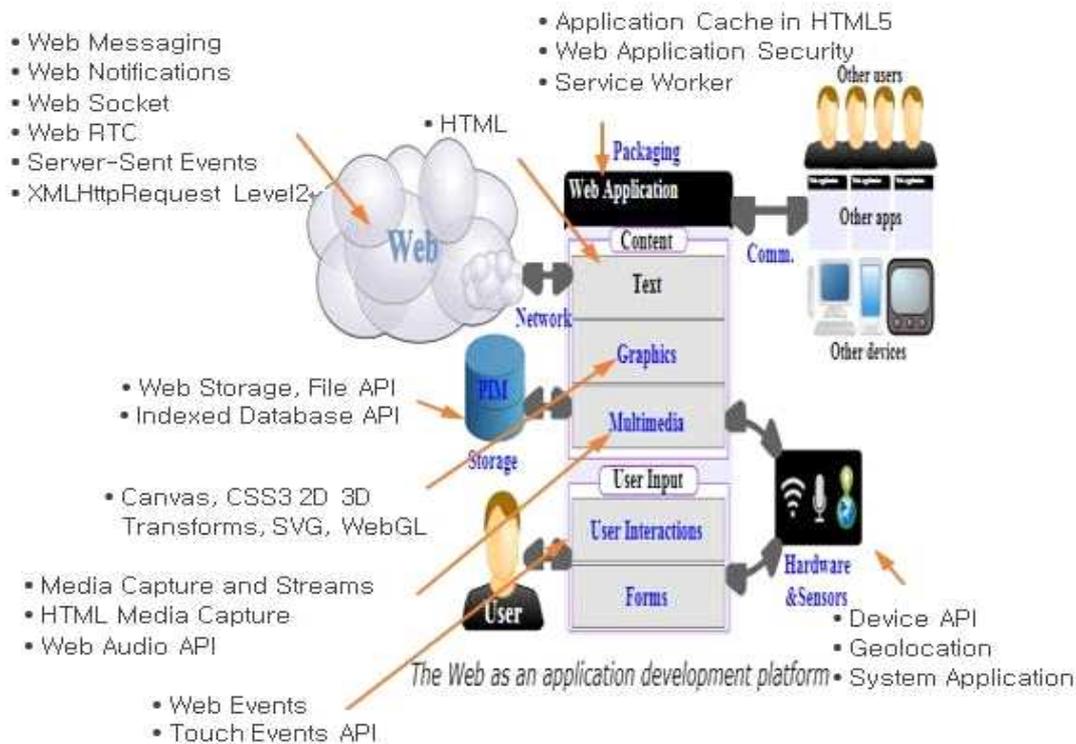
- ☑ 마이크로소프트 Windows10 Edge 브라우저 이후 액티브X 지원 중단
- ☑ NPAPI는 크롬과 파이어폭스에서 2016년 12월 이후 사용 중단(플래시 플레이어는 이용자 선택으로 지원하고 있으나, 크롬은 69버전 이후부터 선택적 사용 기능도 지원 중단)
- ☑ 자바 애플릿은 2017년 3월 JDK9 이상에서 기술 지원 중단
- ☑ 어도비 플래시는 2020년 말 기술 지원 중단 예정(2017년 말 이후 제품 업데이트 중단)
- ☑ 마이크로소프트 실버라이트는 2017년 이후 업데이트 중단 및 Edge 브라우저에서 사용 중단 (2019년부터 Edge 브라우저의 플래시 플레이어 비활성화 예정)

## 플러그인 기술 유형별 분류 요약

구분	기술 유형	플러그인 기술 설명	사용 영역	비고	
1	액티브X	응용 프로그램과 웹 브라우저를 연동하기 위한 기술로 브라우저가 가진 한계인 정적인 UI와 PC자원에 접근하지 못하는 문제를 해결	<ul style="list-style-type: none"> <li>• 본인확인</li> <li>• 전자서명</li> <li>• 전자결제</li> <li>• 보안</li> <li>• 문서출력</li> <li>• 멀티미디어 및 파일처리</li> </ul>	Edge부터 지원중단	
2	EXE(dmg)	EXE(dmg) 실행파일 방식의 경우 URI 프로토콜 핸들러, 브라우저별 익스텐션, 로컬 웹서버 루프백 방식, DLL injection을 통한 메모리 이벤트 모니터링 방식으로 구현	<ul style="list-style-type: none"> <li>• 본인확인</li> <li>• 전자서명</li> <li>• 전자결제</li> <li>• 보안</li> <li>• 문서출력</li> <li>• 멀티미디어 및 파일처리</li> </ul>		
3	RIA	Flash Player (Flex 포함)	Adobe에서 개발한 플러그인으로 동영상 콘텐츠 재생 및 애니메이션, 게임 등 그래픽 가속이 필요한 서비스 구현을 위해 사용	<ul style="list-style-type: none"> <li>• 게임 애니메이션</li> <li>• 멀티미디어</li> <li>• 에디터, 리포팅툴</li> </ul>	2020년 기술지원 중단예정
		Sliverlight	MS사에서 Flash Player와 유사한 기능 제공을 위해 개발한 플러그인	<ul style="list-style-type: none"> <li>• 게임 애니메이션</li> <li>• 멀티미디어</li> <li>• 에디터, 리포팅툴</li> </ul>	2020년 기술지원 중단예정
		Java Applet	자바 가상 머신이 내장된 웹브라우저나 Applet Viewer로 실행할 수 있는 플러그인으로 바이트코드로 실행되어 대부분의 OS와 브라우저 지원	<ul style="list-style-type: none"> <li>• 에디터, 리포팅툴</li> <li>• 게임</li> </ul>	2017년2월 지원중단
		엑스플랫폼	웹 UI(그리드, 차트, 리포트) 및 UX(효과)를 쉽게 저작하고 배포하기 위해 개발한 플러그인	<ul style="list-style-type: none"> <li>• 에디터, 리포팅툴</li> <li>• 그리드, 차트</li> <li>• 애니메이션</li> </ul>	
4	NPAPI(Netscape Plugin Application Programming Interface)	Netscape사에서 액티브X 유사한 기능 제공을 위해 개발한 플러그인으로 윈도우, 유닉스, 맥OS 환경에서 크롬 및 모질라, 사파리 브라우저의 플러그인 지원을 위해 개발	<ul style="list-style-type: none"> <li>• 본인확인</li> <li>• 전자서명</li> <li>• 전자결제</li> <li>• 보안</li> <li>• 문서출력</li> <li>• 멀티미디어, 파일처리</li> <li>• 원격제어 및 장치관리</li> </ul>	2016년 지원중단	
5	기타(Native Client, Web Assembly)	크롬 브라우저에서 인텔 x86, ARM 네이티브 코드를 실행하기 위한 샌드박스 기술로 NPAPI를 대체하기 위해 사용	<ul style="list-style-type: none"> <li>• 어도비 플래시</li> <li>• 내장 PDF 뷰어</li> <li>• 게임</li> <li>• 원격제어 및 장치관리</li> </ul>		

## 4 웹표준 기술(HTML5)

HTML5는 월드 와이드 웹표준(World Wide Web Consortium 이하 W3C)의 핵심 마크업 언어 5번째 버전으로 비디오, 오디오, Rich UI, Web Storage 등 다양한 기능을 플러그인 없이 브라우저만으로 쉽게 사용하는 것을 목적으로 2014년 10월 28일 HTML5 표준안을 확정함(최신 규격은 2017년 12월 14일 제정한 HTML5.2)



| 그림 1 | HTML5 관련 기술 표준 규격(출처 : W3C)

HTML5는 마크업 언어 표준 외에도 아래와 같은 웹 관련 표준 전체에 대한 보통명사로 명시적으로 사용

- W3C 웹표준(즉, 하이퍼텍스트 생성 언어(HTML), 종속형 스타일 시트(CSS), 문서 객체 모델(DOM), XMLHttpRequest(XHR))
- W3C HTML5, CSS3, Web Application 표준
- W3C SVG, MathML3.0과 같은 외부 마크업 언어 표준
- Sensor API 및 시스템 리소스(Web Bluetooth) 표준
- W3C의 WAI-ARIA 와 같은 접근성 향상 기술
- 자바스크립트 표준(ECMAScript라고도 함)

〈표 2〉 HTML5 주요 기능 설명

주요기능	설명	W3C 표준명
웹 폼 (Web Form)	이용자의 다양한 입력 정보를 받기 위해 사용되는 입력 형태에 대한 정의에 사용되는 마크업, 애트리뷰트와 이벤트	HTML5
웹 폰트	이용자가 가지고 있지 않은 일반 폰트를 웹페이지에서 다운로드해서 사용할 수 있는 기술	Web Fonts
그래픽 애니메이션	웹에서 즉시모드(immediate mode)로 2차원 그래픽을 그리기 위한 API와 <canvas>내 각종 객체를 회전, 변환하고 이미지 생성 등 각종 효과를 주는 기능에 대한 API	Canvas 2D Canvas Context
벡터 그래픽	XML 기반의 2차원 벡터 그래픽을 표현하기 위한 언어, SVG(Scalable Vector Graphic)	HTML5
비디오, 오디오	<video>는 비디오 또는 영화를 보여주기 위해 사용되는 미디어 element이며, <audio>는 사운드나 오디오 스트림을 표현하기 위한 미디어 element	HTML5
위치(GPS)	디바이스의 지리적 위치 정보를 제공하는 API	Geolocation API
오프라인 웹 애플리케이션	인터넷 연결이 지원되지 않는 경우에도 웹 애플리케이션이 정상적으로 수행될 수 있도록 지원하는 기능으로 애플리케이션에 대한 캐시와 데이터에 대한 캐시로 구성	HTML5
로컬 스토리지	기존의 쿠키의 기능을 개선하기 위한 목적으로 개발된 기능으로 웹 클라이언트에서 키와 값이 쌍으로 구성된 데이터를 비휘발성으로 저장(브라우저 캐시 삭제시 지워짐)	WebStorage localStorage
백그라운드 웹 서비스	웹페이지나 사용자 인터랙션이 필요하지 않은 기능들을 위한 기회를 제공하고, 웹 페이지와는 별개로 자바스크립트 내에서 Register 등록하고, 브라우저에 의해 백그라운드에서 실행되는 스크립트	Service Worker
파일 업/다운로드	클라이언트에 있는 파일 선택 및 데이터 추출	File API
화상, 음성 통신	웹브라우저 간에 플러그인의 도움 없이 서로 통신(비디오 채팅과 P2P 데이터 공유)할 수 있도록 설계된 Web Real-Time Communications API	WebRTC
TCP 통신	웹 애플리케이션이 서버 측의 프로세스와 직접적인 양방향 통신을 위한 소켓 API	WebSocket API

# III

## 플러그인 제거 방안

1. 개요
2. 본인확인
3. 전자서명
4. 전자결제
5. PC 및 공인인증서 보안
6. 전자문서 조회 및 보안
7. 출력물 위변조 방지 및  
프린터 제어
8. 멀티미디어 및 파일처리 등
9. 기타 플러그인

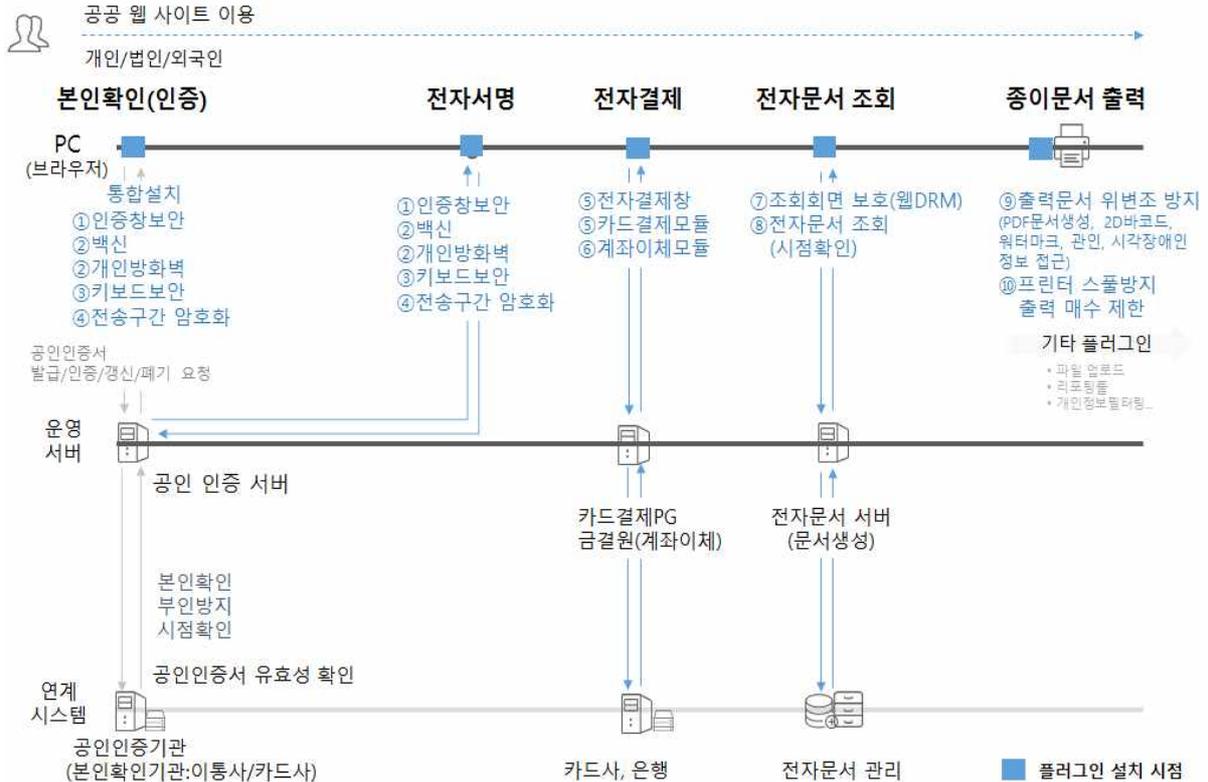
### III. 플러그인 제거 방안

#### 1 개요

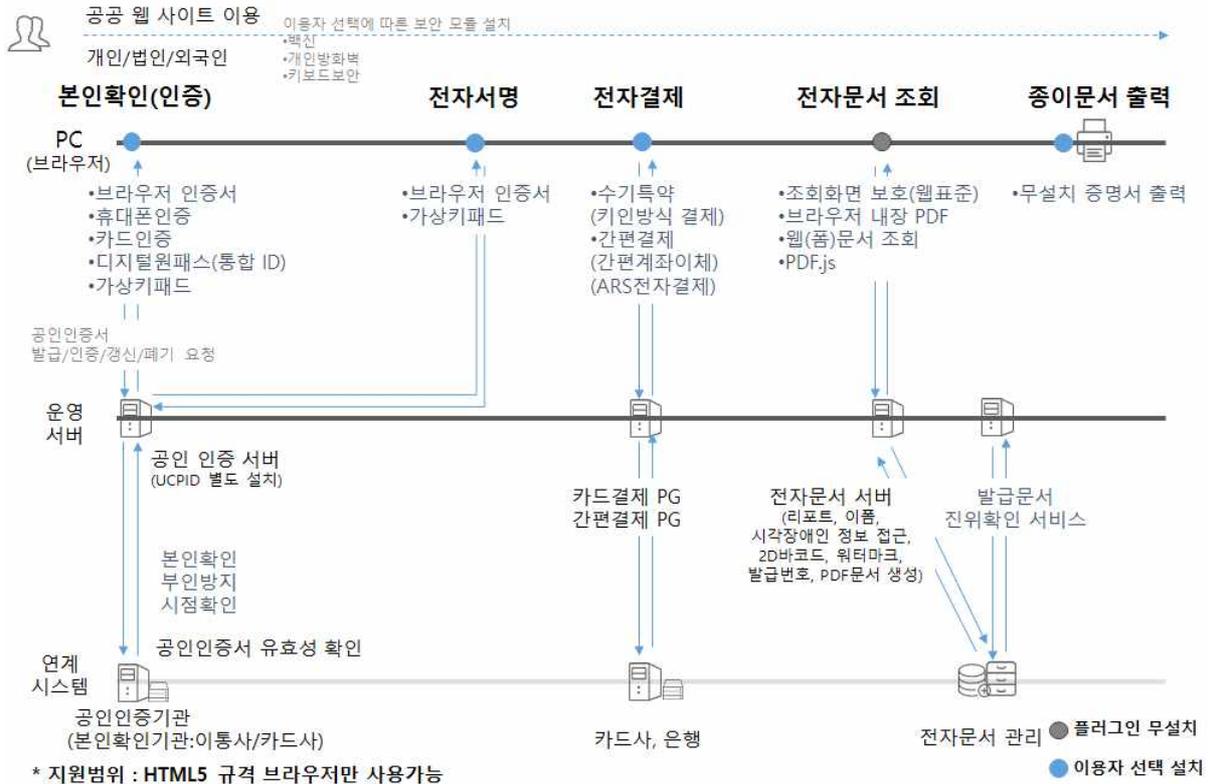
##### 플러그인 제거 원칙

- **최신 웹브라우저만으로 별도의 플러그인 설치없이 웹사이트를 이용할 수 있어야 한다.**
  - 최신 웹브라우저는 IE 11, Edge 12이상, Chrome 50 이상, Firefox 40 이상, Whale 1.0 이상, Safari8.0 이상 등 최신 웹표준(HTML5 등)을 지원하는 웹브라우저를 말함 (브라우저 userAgent를 구분을 통해 OS, 브라우저 이름, 버전 확인 후 웹서비스 제공)
  - 이용자가 웹사이트에서 PC로 다운로드한 콘텐츠를 열람하기 위한 SW는 플러그인이 아님 (예시: HWP 파일 열람을 위한 문서뷰어SW, MP4 파일 재생을 위한 동영상 재생SW, ZIP파일 압축해제를 위한 압축해제SW 등)
- **최신 웹표준을 지원하지 않는 웹브라우저 이용자는 플러그인을 설치하여 웹사이트를 이용할 수 있다.**
  - 최신 웹표준을 활용하여 구현된 웹서비스는 최신 웹표준을 지원하지 않는 브라우저 이용자는 사용이 불가하므로, 동일 기능을 기존의 플러그인 방식으로 서비스 제공 가능 (동일한 기능을 플러그인 방식과 웹표준 방식으로 병행 제공 가능)
  - 이용자의 PC에 기존의 플러그인이 설치되어 있는 경우, 이용자는 해당 플러그인을 활용하여 웹사이트 이용 가능
- **플러그인 사용을 원하는 이용자는 플러그인을 설치하여 웹사이트를 이용할 수 있다.**
  - 백신, 방화벽 등 웹표준으로 대체가 곤란한 플러그인에 한해 이용자가 설치를 원하는 경우에 설치되도록 제공
  - 플러그인 설치여부를 선택할 때, 이용자에게 플러그인을 설치하도록 강제하지 않음
    - ⚙️ 이용자가 명시적으로 설치를 동의하기 전까지 설치 금지(옵트인 방식)
  - 서비스 흐름을 방해하지 않도록 플러그인 설치 여부선택 UI 구성
    - ⚙️ 팝업이나 다이얼로그 방식의 선택 UI 지양
  - 웹사이트의 첫 페이지에서 일괄 설치하지 않고, 해당 플러그인의 기능이 필요한 시점에 설치

## 플러그인 사용 목적별 사용현황 및 제거방안



| 그림 2 | 현재 플러그인 사용 목적별 설치 현황(AS-IS)



| 그림 3 | 주요 플러그인 사용 목적별 제거 방안(TO\_BE)

## 플러그인 제거방식 요약

	플러그인 유형	제거 방안	비고
1	공인인증서	<ul style="list-style-type: none"> <li>전자서명 : 브라우저 인증서</li> <li>본인확인 : 휴대폰 본인확인, 신용카드 본인확인, 브라우저 인증서, 디지털 원패스</li> </ul>	<ul style="list-style-type: none"> <li>브라우저 인증서 도입 시 금융결제원의 공동저장소 연동 권장</li> </ul>
2	백신, 개인방화벽	<ul style="list-style-type: none"> <li>이용자 선택 설치</li> <li>효과성을 재검토하여 제거</li> </ul>	<ul style="list-style-type: none"> <li>플러그인 설치를 유도(강제) 하지 않는 웹페이지 UI 구성</li> </ul>
3	키보드보안	<ul style="list-style-type: none"> <li>가상키패드</li> <li>이용자 선택 설치</li> <li>효과성을 재검토하여 제거</li> </ul>	<ul style="list-style-type: none"> <li>입력 정보가 많은 경우 가상키패드는 이용 불편</li> </ul>
4	전송구간 암호화	<ul style="list-style-type: none"> <li>SSL(Secure Socket Layer)적용</li> </ul>	<ul style="list-style-type: none"> <li>전자서명이외에도 운영 웹페이지에도 SSL 적용 가능</li> </ul>
5	신용카드 전자결제	<ul style="list-style-type: none"> <li>키인 방식 카드결제(수기결제)</li> <li>카드간편결제 or ARS 전자결제</li> </ul>	<ul style="list-style-type: none"> <li>키인 방식 서비스 개발방식의 경우 전자결제 페이지 개발 필요</li> <li>카드간편결제 도입 시 기존 PG 계약 기간 및 해지 요건 확인</li> </ul>
6	계좌이체 전자결제	<ul style="list-style-type: none"> <li>간편계좌이체 결제</li> </ul>	<ul style="list-style-type: none"> <li>간편계좌이체 도입 시 기존 PG 계약 기간 및 해지 요건 확인</li> </ul>
7	조회화면 보호 (웹 DRM)	<ul style="list-style-type: none"> <li>효과성을 재검토하여 제거</li> <li>웹표준 조회화면보호 적용                             <ul style="list-style-type: none"> <li>- 자체 개발 적용</li> <li>- 웹표준 솔루션 도입</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>화면 보호 기능에 한계가 있음</li> <li>웹표준 개발 시 일부 기능 지원 불가(메뉴제어, 소스보기)</li> <li>클라이언트와 서버에서 입력 데이터 유효성 검증 코드 추가</li> </ul>
8	전자문서 조회	<ul style="list-style-type: none"> <li>웹표준 웹폼 문서 뷰어 솔루션 도입(시점확인 기능 없음)</li> <li>서버에서 PDF 변환 솔루션을 통해 PDF 문서 생성 후 브라우저 내장 PDF 뷰어로 조회</li> </ul>	<ul style="list-style-type: none"> <li>시점확인 기능이 필요할 경우 PDF 변환 솔루션을 통해 지원</li> <li>IE9~11은 내장PDF 뷰어가 없어 Acrobat Reader 사전 설치 필요</li> </ul>
9	출력문서 위변조 방지	<ul style="list-style-type: none"> <li>서버 변환 방식 출력문서 위변조 방지(복사방지마크, 전자관인, 2차원 바코드, 진위확인번호) 솔루션 도입</li> <li>발급문서 진위확인서비스 도입</li> </ul>	<ul style="list-style-type: none"> <li>2차원 바코드 방식은 진위확인번호 방식에 비해 진위확인절차가 불편</li> </ul>
10	프린터 스펙 접근제어 및 출력 매수 제한	<ul style="list-style-type: none"> <li>증명서 무료화 유도를 통해 제거</li> </ul>	<ul style="list-style-type: none"> <li>IE에서 웹폼, 웹페이지 출력 시 하단 URL이 노출(PDF 변환 후 출력 시 비노출 가능)</li> </ul>

 원격제어, 장치관리, 인증서 모바일 복사 플러그인은 이용자 선택 설치

## 2 본인확인

### 개요

웹사이트 회원(개인, 법인)가입, 비밀번호 변경, 게시판 글쓰기 등에서 실제 본인 여부 확인과 실명확인을 하기 위해 공인인증서를 이용

개인 및 법인의 본인확인과 전자서명을 하나의 솔루션으로 처리하기 위해 대부분 공인인증서를 본인확인 및 본인인증 방법으로 사용(현재 법인의 전자적 본인확인 방법은 공인인증서를 이용한 방법 외에는 없음)

만14세 미만 이용자의 회원 가입 시 미성년 이용자의 개인정보를 처리하기 위해 법정대리인의 동의를 위해 공인인증서(본인확인 및 가입여부) 사용

본인인증은 이미 본인확인을 통해 해당 웹사이트에 본인의 인증정보를 등록한 상태에서 서비스 이용을 위해 가입 여부를 확인(로그인)하는 절차로 대부분 아이디/패스워드나 공인인증서 비밀번호 입력 방식 사용



| 그림 4 | 회원 가입 유형 및 본인확인 후 가입 절차(출처 : 잡월드 가입화면)

- ☞ 실명확인 : 이름(법인)과 주민등록번호(사업자등록번호)에 대해 실제 식별 번호 존재 여부 및 이름과 번호 일치 여부 확인
- ☞ 본인확인 : 특정한 방법을 통하여 특정인이 본인인지 아닌지를 식별하는 방법이나 수단
- ☞ 본인인증 : 온라인 이용자가 웹사이트 회원가입, 비밀번호변경, 게시판 글쓰기 등과 같은 서비스 이용시 실제 본인인지 여부를 휴대폰, 공인인증서 등의 본인확인수단을 통해 확인하는 방법으로 통상적으로 본인확인과 혼용되어 사용

## 플러그인 사용 현황

본인확인을 위한 플러그인은 공인인증서 사용에 따른 전자서명창 보안, 전송구간 암호화, 키보드보안 플러그인 사용

### ■ 전자서명창 보안

- 공인인증서 사용을 위한 인증서 파일 접근 및 이용자 PC와 웹 구간(인증센터)암호화를 통한 기밀성, 무결성, 부인방지를 위한 전자서명용 프로그램

### ■ 전송구간 암호화

- PC 웹브라우저에서 서버, 또는 서버에서 서버로 전송하는 데이터를 안전하게 암호화 하는 프로그램

### ■ 키보드보안

- 백도어 또는 해킹툴에 의한 키 입력 가로채기, 후킹(Hooking), 상용 키로그 무력화를 통한 정보 유출을 방지하기 위해 설치하는 프로그램

## 전자서명창 대체 방안

본인확인용은 기존 공인인증서를 사용하는 본인 확인 방법뿐만 아니라 웹사이트 운영 기관 선택에 따라 플러그인이 필요 없는 휴대폰 본인확인 및 신용카드 본인확인, 디지털 원패스(통합 ID), 브라우저 인증서 등을 사용하여 전환 가능

본인확인 수단은 전자서명창, 전송구간 암호화를 플러그인 없이 이용할 수 있음

〈표 3〉 본인인증 또는 실명인증을 위한 방법

	본인확인수단	본인인증	실명인증	법인지원여부	구현복잡도	운영기관 비용
1	휴대폰 인증	○	○	지원안함	낮음	유료 (건당과금)
2	신용카드 인증	○	○	지원안함	낮음	유료 (건당과금)
3	브라우저인증서	○	○	추후지원	중간	유료 (솔루션도입비)
4	디지털 원패스 (통합 ID)	○	○	지원안함	중간	무료 (일부 개발비)

☀ PC백신, 개인방화벽, 키보드보안은 이용자 선택 설치 가능

〈표 4〉 본인확인 수단 별 현황

본인확인수단	인증방식	가입정보	개인식별정보	인증서비스 지원기관	연동방식
휴대폰	생년월일 기반	성명, 성별, 생년월일, 휴대폰번호	사업자 간 이용자 식별연계정보(C.I), 중복가입확인정보(D.I)	휴대폰 본인확인기관	웹페이지, 소켓방식
신용(체크)카드	생년월일 기반	생년월일, 카드번호, 유효기간, 비번2자리	C.I, D.I	신용카드 본인확인기관	웹페이지, 소켓방식
브라우저인증서	인증서 비밀번호	인증서 비밀번호	C.I, D.I	공인인증기관	인증서버연동 규격

☀️ 본인확인 사업자 현황

- 공인인증기관 : 금융결제원, 코스콤, 한국정보인증, 한국전자인증, KTFNET, 이니텍
- 휴대폰 본인확인기관 : SKT, KT, LGU+
- 신용카드 본인확인기관 : 삼성, 현대, 국민, 롯데, 비씨, 신한, 하나카드
- 아이핀 인증기관 : NICE, SCI, KOB

☀️ C.I(Connecting Information), D.I(Duplication Information)

- 본인확인기관이 운영기관에게 전달하는 주민등록번호를 대체하는 고객 식별(key) 값

본인확인 수단을 이용자가 선택할 수 있도록 본인확인 서비스를 지원할 경우, 본인확인 방법을 선택할 수 있는 웹 화면 구성 필요

본인인증

• 회원가입을 위한 다양한 본인인증수단을 선택하실 수 있습니다.  
 • 만 14세 미만 아동의 회원가입은 법정대리인의 동의를 위하여 휴대전화 인증을 선택하시기 바랍니다.  
 • 모든 본인인증방법에 해당사항이 없으면 가까운 세무서 민원봉사실을 방문하시기 바랍니다.

STEP.1 회원유형선택	STEP.2 본인인증	STEP.3 이용약관 동의	STEP.4 회원정보 확인 및 수정	STEP.5 가입완료
------------------	----------------	-------------------	------------------------	----------------

• 본인의 신원을 확인할 수 있는 방법이 있습니까?



공인인증서



휴대전화



신용카드

• **사용불가 휴대전화**  
 - 주민등록번호 명의로 등록된 휴대전화번호 사용가능, 사업자번호 명의로 법인은 인증불가  
 - 연체폰이나 선불폰일 경우에는 인증불가

• **사용불가 신용카드**  
 - 주민등록번호 명의로 등록된 신용카드 사용가능, 사업자번호 명의로 법인은 인증불가

| 그림 5 | 다양한 본인확인 선택 화면(출처 : 홈택스)

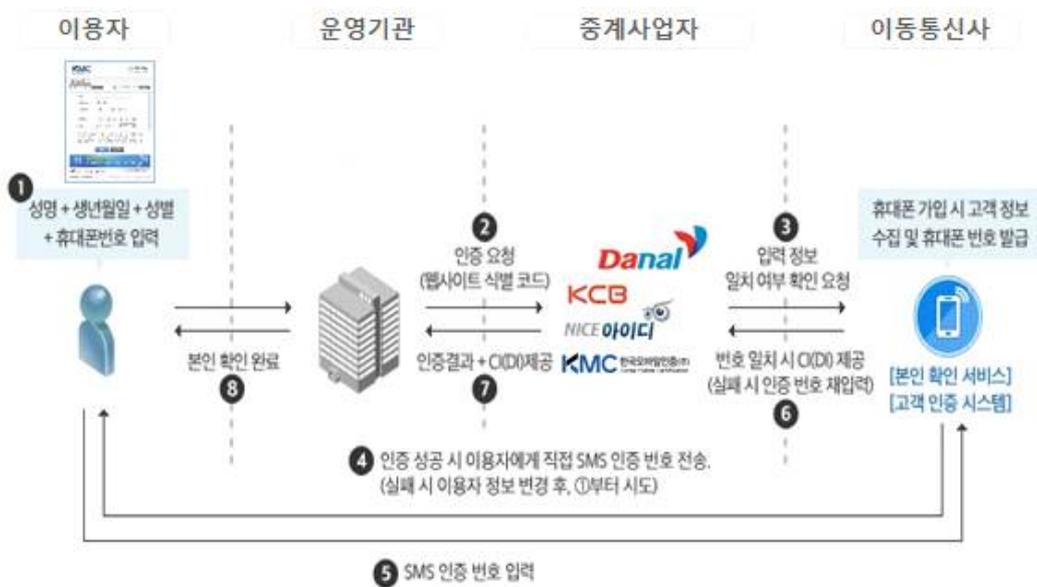
☀️ 아이핀(i-Pin)의 경우 현재(2018.09) 키보드보안 플러그인 설치 필요

## ■ 휴대폰 본인확인

### 🔗 기술 개요

휴대폰 본인확인기관과 중계 사업자가 제공하는 웹페이지에 개인정보(이름, 성별, 생년월일, 이동통신사, 휴대폰번호, 이동통신사가 제공하는 승인번호를 입력)을 입력하면 본인확인기관을 통해 본인여부 확인결과와 성인 여부, 남녀 성별, 외국인 여부 등의 정보확인 지원

휴대폰 본인확인은 회원가입, 비밀번호 관리, 실명확인 게시판 글쓰기, 상품 구매 등에서 활용



| 그림 6 | 휴대폰 본인확인 서비스 FLOW

### 🔗 적용 방법

- 본인확인 방식은 웹페이지 링크 호출 방식과 소켓 방식으로 제공(대부분 웹페이지 링크 호출 방식 사용)
- 소켓방식은 입력 받은 개인정보와 운영기관 정보를 사전 정의된 연동 규격에 따라 본인확인기관에 전송하고 결과값(반환코드)을 운영기관이 확인하는 방식
- 전년도 본인확인 건수 확인을 통해 예산 편성(중계사업자 협의)
- 중계사업자와 휴대폰 본인확인 도입 가맹점 계약 및 수수료 계약
- 중계 사업자를 통해 본인확인 서비스용 자바스크립트 라이브러리와 가맹점 식별 코드(사용료 정산용) 수령

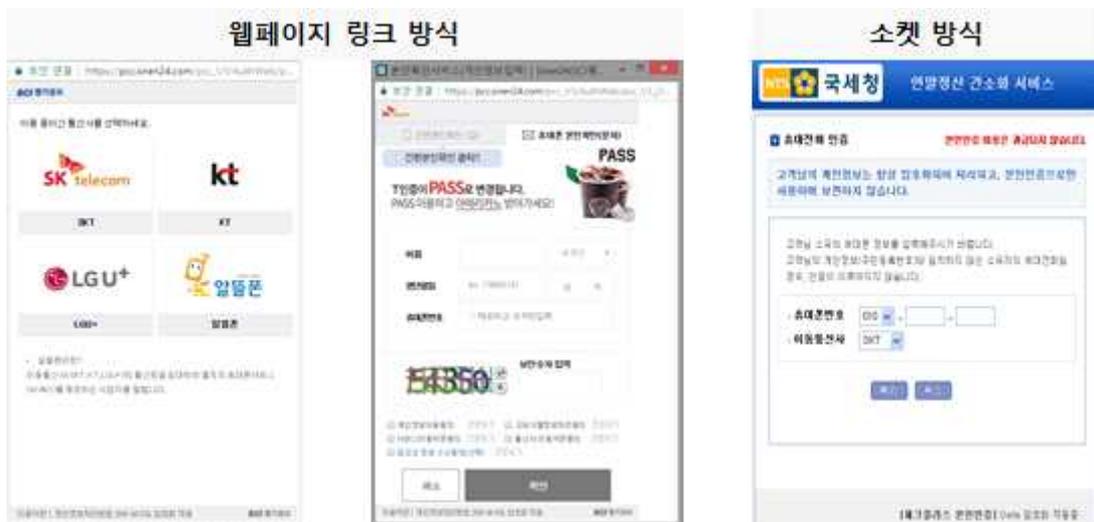
- 본인확인이 필요한 웹 페이지에 본인확인 호출용 자바스크립트 라이브러리 및 인증 페이지 호출코드 추가
- 본인확인(중계) 기관과 가맹점 계약 후 전달 받은 가맹점 식별코드(사용료 정산)를 추가하고 본인확인 인증 페이지 호출 및 이용자에게 입력 받은 데이터를 전달 테스트
- 반환된 결과값을 통한 본인확인 및 실명확인
- 조회한 인증정보에서 고객 정보를 추출 후 실명 확인 및 기존 가입 여부 확인 후 서비스 FLOW에 따라 페이지 이동

### 🔗 도입 시 유의사항

- 중계사업자 중 키보드보안 플러그인 설치없이 본인확인 웹페이지를 적용하는 사업자 선정(본인확인화면의 스크립트 난독화 및 전송구간암호화 같은 보안 조치 적용 여부 확인)
- 운영기관이 공개 인터넷망을 연결할 수 없거나, 자체 본인확인 제공이 필요할 경우 소켓방식으로 제공(소켓방식의 경우 이동통신사의 사전승인절차 필요)
- 알뜰폰을 지원하는 본인확인 중계사업자 선택
- 조회 건수(정산 비교) 확인이 필요한 경우 CI, DI 리턴 값에 대한 로그관리시스템 개발 필요

### 🔗 적용 사례

- 공공, 쇼핑몰, 은행, 보험, 증권 웹사이트에서 본인확인 방법으로 사용



| 그림 7 | 휴대폰 본인확인 서비스 예시

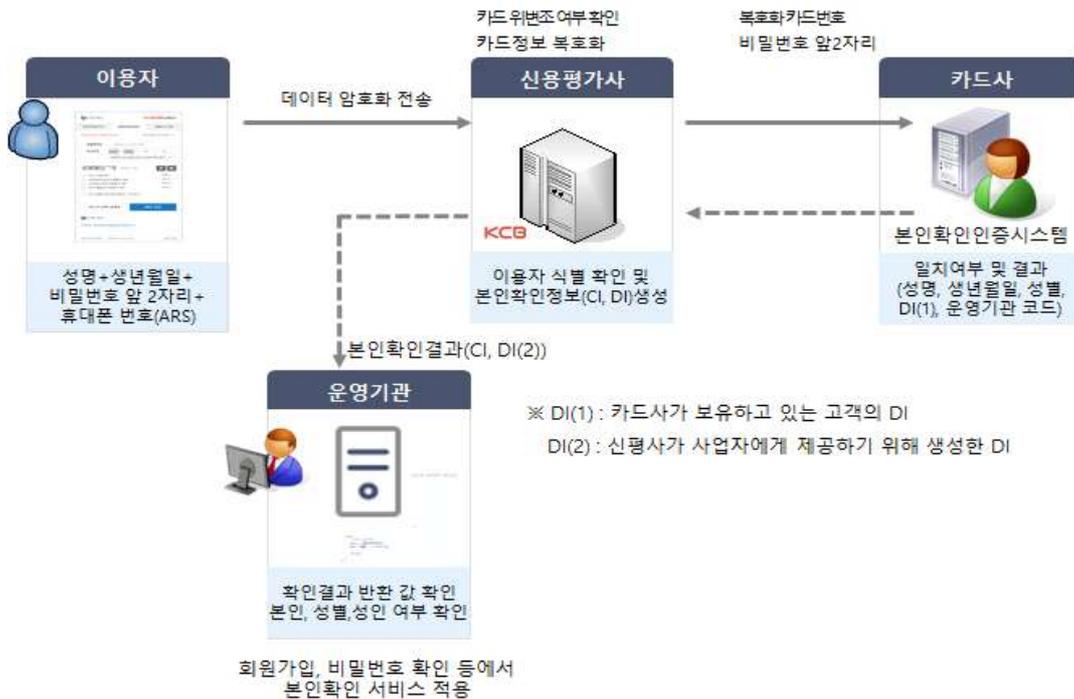
## ■ 신용카드 본인확인

### 🔗 기술 개요

신용카드 본인확인은 본인 명의의 카드를 보유한 이용자의 본인확인 방법으로 활용 가능하며, 본인확인 기관의 신용(체크)카드 발급 정보를 기반으로 아래와 같은 방식으로 본인확인 서비스 제공

- ▶ 스마트폰 앱 카드 실행
- ▶ 카드사 홈페이지 접속 후 비밀번호 입력
- ▶ 웹페이지에 정보 입력 후 휴대전화 ARS 연결 확인

휴대폰 본인확인과 유사하게 개인 정보(이름, 생년월일, 카드번호, 비밀번호 2자리) 입력 후 휴대폰 ARS를 통해 인증번호를 입력하는 방식으로 사용(본인여부 확인 결과와 나이, 성별 정보 제공)



| 그림 8 | 신용카드 방식 본인확인 서비스 FLOW

### 🔗 적용 방법

- 신용카드 본인확인 도입 방식 선택(웹페이지 정보 입력 + ARS 확인 방식)
- 중계사업자(신평사)와 신용카드 본인확인 도입 가맹점 계약 및 수수료 계약

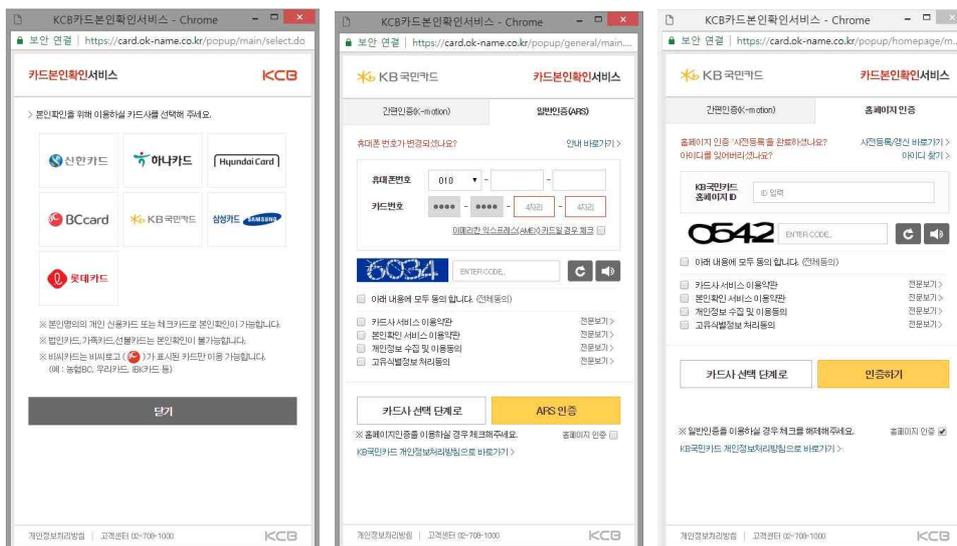
- 본인 확인 서비스용 자바스크립트 라이브러리와 가맹점 식별코드 (사용료 정산용) 확인
- 본인확인이 필요한 웹페이지에 본인확인 호출용 자바스크립트 라이브러리 및 인증 페이지 호출코드 추가
- 중계사업자와 가맹점 계약 후 전달 받은 가맹점 식별코드(사용료 정산)를 추가하고 본인확인 인증 페이지 호출 및 이용자에게 입력 받은 데이터를 전달 테스트
- 본인확인 데이터로 반환된 결과값을 통한 본인확인 및 실명확인
- 조회한 인증정보에서 고객 정보를 추출 후 실명 확인 및 기존 가입 여부 확인 후 서비스 FLOW에 따라 페이지 이동

### 🔗 도입 시 유의사항

- 법인카드, 가족카드, 선불카드 본인확인 불가(법인 본인 확인 불가)
- 조회 건수(정산 비교) 확인이 필요한 경우 CI, DI 리턴 값에 대한 로그관리시스템 개발 필요

### 🔗 적용 사례

- 이베이코리아 지마켓, 옥션(성인 인증), 한게임(성인 인증)



| 그림 9 | 비회원 카드 본인확인 및 성인인증(출처 : 옥션 비회원인증)

### ■ 브라우저 인증서

본문 중 “3. 전자서명 중 브라우저 인증서” 내용 참조

## ■ 디지털 원패스(통합 ID)

### 🔗 기술 개요

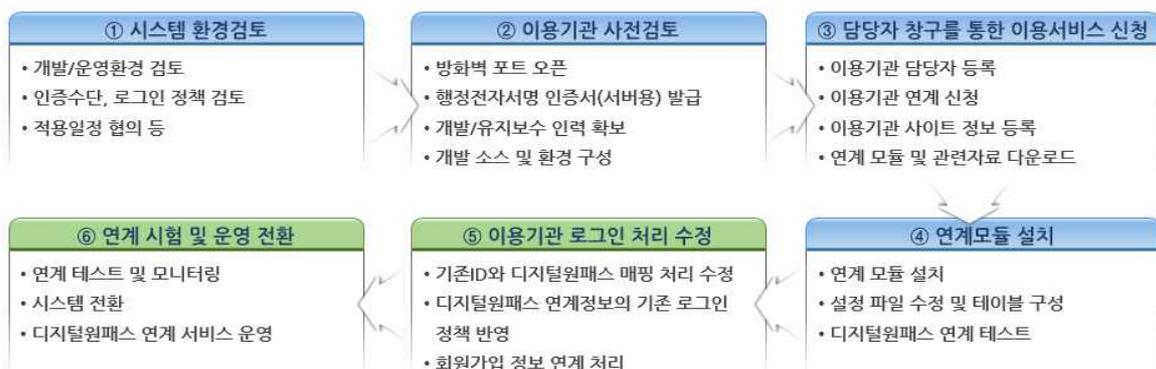
정부 및 외부 신뢰된 인증기관의 인증수단 및 인증수준을 선택하여 본인이 생성한 본인 인증 정보를 디지털 원패스에 등록하여 편리하게 인증절차를 간소화하는 서비스로 운영기관 웹서비스 이용 시 웹서비스 마다 아이디를 일일이 기억할 필요 없이 하나의 디지털 원패스 아이디를 통해 여러 대민용 웹서비스들을 이용할 수 있도록 통합 로그인 인증 수단(통합 ID)을 제공



| 그림 10 | 디지털 원패스 서비스 개념도

디지털 원패스를 도입한 대민용 웹사이트는 통합인증포털에서 제공한 디지털 원패스 인증프레임워크 연계 배포 모듈(API)을 운영기관의 서버에 탑재하여 이용자에게 디지털 원패스 본인확인 및 본인인증(로그인) 서비스 제공

### 🔗 적용 방법



| 그림 11 | 디지털 원패스 도입 기관 적용 절차

- 대민용 웹사이트 운영기관은 디지털 원패스 도입 사전 협의
- 기존 시스템 개발 유지보수업체를 통해 사전 연계 협의 시 운영기관 시스템 환경 검토

- 운영기관 방화벽 및 개발(인력, 시스템 환경) 관련 사전 준비 진행
- 서비스 신청 및 연계모듈(API), 개발가이드, 샘플코드, 기술교육 자료 검토
- 운영기관 서버에 디지털 원패스 인증 프레임워크 연계 모듈(API) 설치(전자 정부 프레임워크 3.0 기반 설치 사양 제공) 및 회원 테이블 구성
- 디지털 원패스 표준 UI 적용을 위한 웹 소스 및 연계 테스트(사이트 적용 및 개발은 개발유지보수 업체가 수행)
- 기존 운영기관 회원정보 ID(회원 DB Table) 체계와 디지털 원패스 본인 인증(ID) 체계 매핑 처리 연계 개발(필요시)
- 연계 API를 이용하여 디지털 원패스 인증정보 연계 시험 및 운영 연동 테스트(통합 ID로 로그인 처리)
- 사업자 회원 가입 본인확인, 로그인 웹 페이지에 디지털 원패스 연계 서비스 운영(서비스 런칭)

#### 도입 시 유의사항

- 회원 가입 시 일회성 본인확인 용도로는 지원하지 않음(비회원서비스를 위한 본인확인은 지원)
- 운영기관의 기존 ID와 디지털 원패스 ID 매핑을 위한 개인식별정보(CI)가 존재하지 않을 경우, 디지털 원패스 담당자와 회원 매핑 정책 검토 필요
- 디지털 원패스 도입 이후에도 운영기관 선택에 따라 기존 회원가입 정책 유지 가능(이용자 선택에 따라 디지털 원패스 or 기존 가입방식)
- 디지털 원패스의 본인확인 및 로그인 수단은 아래와 같음

〈표 5〉 디지털 원패스 본인확인 및 로그인 수단

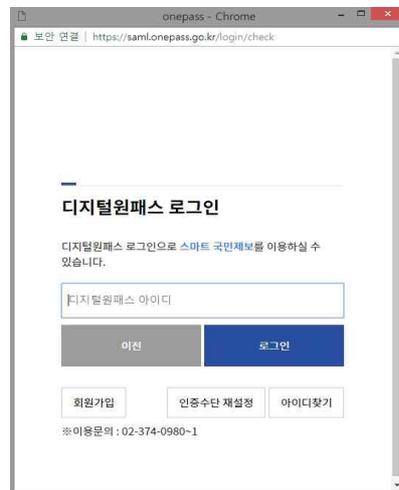
구분	방법	기능설명
회원가입 (본인확인 수단)	휴대폰 본인확인	본인이 소유한 휴대폰번호 등을 입력하여 통신사 가입정보와 일치여부 확인 (전용앱 또는 SMS)
	공공아이핀	본인이 가입한 아이핀계정을 활용하여 인증
	신용카드 인증 (19년 예정)	본인이 소유한 신용카드정보 등을 입력하여 카드사 발급정보와 일치여부 확인 (전용앱 또는 ARS)

로그인 수단	패스워드	사용자가 설정한 비밀번호를 입력하여 인증
	SMS 인증	사전에 등록된 휴대폰 문자메세지(SMS)로 전송한 1회용 인증코드를 입력하여 인증
	Email 인증	사전에 등록된 이메일로 전송한 1회용 인증코드를 입력하여 인증
	지문	모바일 앱을 활용하여 지문 입력을 통한 인증
	PC 인증서	PC에 저장된 공인인증서를 호출하여 인증
	모바일 인증서(예정)	모바일 앱에 저장된 공인인증서를 호출하여 인증 (비밀번호를 대신해 지문 등 FIIDO 활용)
	안면 또는 홍채(예정)	모바일 앱을 활용하여 안면 또는 홍채 인식을 통한 인증
	PIN(예정)	모바일 단말에서 0~9 까지의 번호로 구성된 간편 비밀번호 입력
패턴(예정)	모바일 단말에서 패턴인식을 이용한 인증	

☀ 생체인증(지문 등)은 단말기 자체의 인증결과를 활용하며, 생체정보를 수집하지 않음

## 🔗 적용 사례

- 경찰청 스마트 국민제보, 국토교통부 교통안전공단 통합페이지 등에 적용



| 그림 12 | 경찰청 스마트 국민제보 디지털 원패스 적용 화면

### 3 전자서명

#### 개요

전자서명은 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는 데 이용하기 위해 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보

전자서명은 전자문서의 서명자 식별, 신원확인, 문서내용의 위·변조 방지, 거래(결제)사실에 대한 부인방지, 정보 노출 방지 등을 위해 사용

전자인증서는 사용자의 신원 등을 확인하기 위한 전자서명키를 담고 있는 파일로, 공인인증기관에서 보증한 공인인증서와 개별기관에서 보증한 사설인증서가 있음  
전자서명에 사용하는 전자인증서는 아래와 같은 정보가 암호화되어 저장됨

〈표 6〉 전자인증서 주요 내용

주요 구성 요소	설명
일련번호	인증서 일련번호
발행기관 식별명칭	인증기관 식별명칭
유효기간	인증서 유효기간 시작일과 만료일
소유자 식별명칭	인증서 소유자의 실명을 포함한 식별명칭
공개키	인증서 소유자의 공개키
공개키 사용목적	공개키의 사용목적을 명시(전자서명, 암호화 등)
인증서 정책	인증서 발행기관이 인증서를 발행하는데 적용한 인증서 정책과 인증업무 준칙을 명시
발행기관의 서명값	인증서 내용이 진실임을 증명하는 발행기관의 전자서명 값

## 플러그인 사용 현황

전자서명을 위한 플러그인은 공인인증서 사용에 따른 전자서명창 보안, 전송구간 암호화, 키보드보안 플러그인 사용

### ■ 전자서명창 보안

- 공인인증서 사용을 위한 인증서 파일 접근 및 이용자 PC와 웹 구간(인증센터)암호화 지원을 통한 기밀성, 무결성, 부인방지를 위한 전자서명용 프로그램

### ■ 전송구간 암호화

- PC 웹브라우저에서 서버, 또는 서버에서 서버로 전송하는 데이터를 안전하게 암호화 하는 프로그램

### ■ 키보드보안

- 백도어 또는 해킹툴에 의한 키 입력 가로채기, 후킹(Hooking), 상용 키로그 무력화를 통한 정보 유출을 방지하기 위해 설치하는 프로그램

## 대체 방안

### ■ 브라우저 인증서(브라우저 로컬 스토리지 인증서 저장·사용방식)

#### 🔗 기술 개요

웹표준(HTML5)을 지원하는 브라우저의 로컬 스토리지 영역에 공인·사설인증서를 저장하여 사용하는 방식으로, 별도의 플러그인 없이 본인확인이나 전자서명 기능을 이용할 수 있음

공인인증서를 브라우저 로컬 스토리지에 직접 발급받아 사용하거나 저장장치(하드디스크, USB 등)에 저장되어있는 공인인증서를 웹표준 전자서명창을 통해 브라우저 로컬 스토리지 영역에 복사해서 사용

대부분의 브라우저 인증서 솔루션은 SSL 전송구간 암호화, 가상키패드 기능을 패키지로 제공

⚙️ 사설인증서의 경우 솔루션 업체에 지원 여부 확인 필요

〈표 7〉 브라우저 인증서 종류

구분	인증서 발급처	주요 기능 설명
직접 발급 방식 (금융결제원 공동저장소 방식)	현재는 금융결제원만 발급	<ul style="list-style-type: none"> <li>• 웹표준(브라우저) 전자서명창에서 직접 발급, 브라우저 로컬 스토리지에 저장(인증서 유효기간 3년)</li> <li>• 공동저장소를 사용할 경우 동일 브라우저에서 서로 다른 웹사이트 간 인증서를 공유 사용할 수 있음</li> <li>• 브라우저에서 하드디스크, USB로 이동/복사 불가</li> </ul>
복사 사용 방식	공인인증기관	<ul style="list-style-type: none"> <li>• 하드디스크나 USB에 저장된 공인인증서를 브라우저 로컬 스토리지 영역에 복사(기존 발급 인증서 유효기간)</li> <li>• 브라우저에서 하드디스크, USB로 이동/복사 가능</li> </ul>

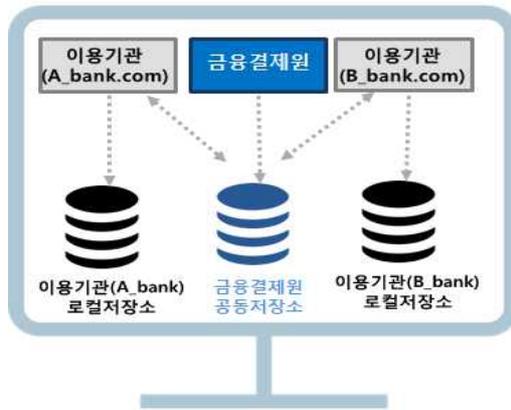
복사사용방식은 아래와 같은 불편이 발생할 수 있음

- 브라우저 인증서는 브라우저의 웹사이트별 로컬 스토리지에 저장되어, 서로 다른 웹사이트에서 동일한 브라우저 인증서를 이용할 수 없고 웹사이트별 인증서(복사본)가 필요
- 브라우저 인증서는 브라우저 캐시(Cache)를 삭제하면 인증서도 함께 삭제됨
  - 인터넷 익스플로러 : 검색 기록 삭제
  - 크롬 : 인터넷 사용 정보 삭제
  - 파이어폭스 : 쿠키, 캐시 삭제
  - 사파리 : 캐시 비우기
- 브라우저 로컬 스토리지의 물리적 위치가 달라 브라우저 별로 공인인증서를 복사하고 이용해야 함(브라우저 인증서 제공 시 브라우저 인증서 사용 안내 및 브라우저 별 웹사이트 저장 안내 필요)

위와 같은 불편을 제거하기 위해 금융결제원의 공동저장소 연계 사용 권장

### ○ 금융결제원의 공동저장소 개념

- 브라우저 인증서 도입 시 금융결제원의 공동저장소 기능을 적용할 경우 각 웹사이트에서 인증서 공동 활용 가능
- 브라우저 공동저장소는 저장기능만 제공하고, 초기 이용 시 공동저장소에 저장된 인증서를 각 사이트별 운영기관 저장소에 복사·사용

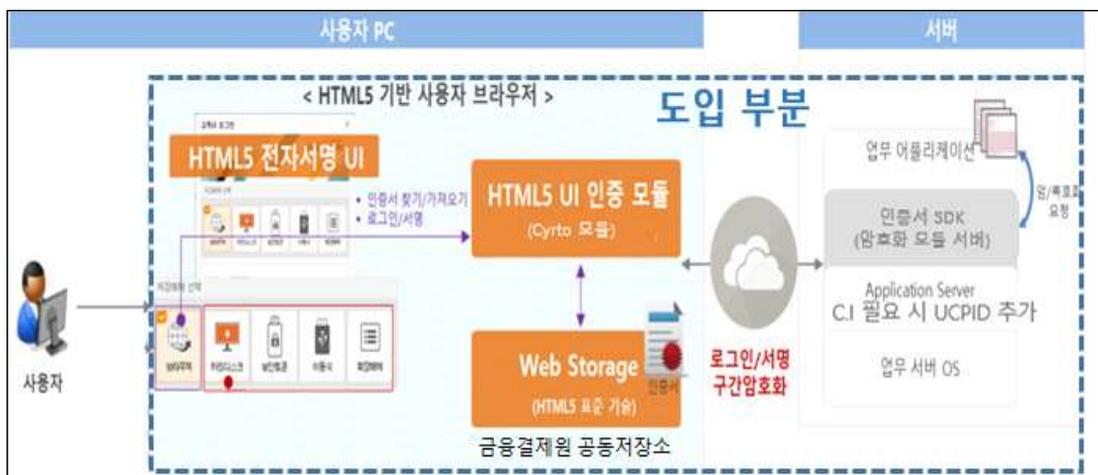


| 그림 13 | 금융결제원 공동저장소 개념도

복사사용 방식 불편사항	브라우저 공동인증서비스
<ul style="list-style-type: none"> <li>☑ 기존 인증서를 브라우저 로컬 스토리지로 복사 불편</li> <li>☑ 웹사이트별 인증서 개별 사용</li> <li>☑ 웹브라우저 캐시 삭제에 따른 인증서 삭제</li> </ul>	<ul style="list-style-type: none"> <li>☑ 브라우저 인증서로 직접 발급(재발급)</li> <li>☑ 브라우저인증서 공동저장소 서비스 제공</li> <li>☑ 인증서 (서버)보관 서비스 제공(예정)</li> </ul>

### 🔗 적용 방법(금융결제원의 공동저장소 연계)

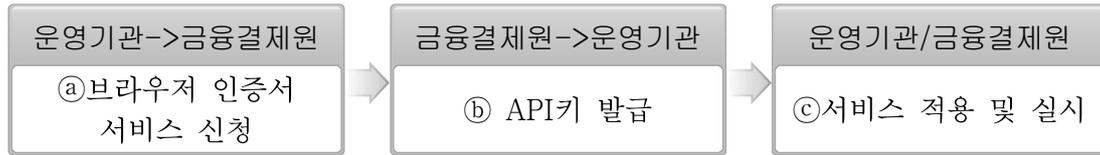
브라우저 인증서는 개인 이용자가 HTML5를 지원하는 PC 브라우저 및 모바일 웹 브라우저에서 공동저장소 적용을 위한 개발자 API 적용을 통해 제공 가능



| 그림 14 | 브라우저 인증서 솔루션 구성

- 브라우저 인증서 및 공동저장소 서비스 신청

- 운영기관은 공동저장소 이용을 위해 연동테스트 신청서를 작성하여, 금융결제원에 브라우저 인증서 및 공동저장소 서비스 신청



- 금융결제원은 서비스 등록 및 운영기관에 테스트, 상용 API 키 발급
- 운영기관과 금융결제원은 서비스 적용 및 모니터링 실시

- 브라우저 인증서 도입

- 브라우저 인증서 공급 솔루션(인증서 발급관리, 인증서버) 업체를 통해 인증 클라이언트 및 서버 솔루션 설치

- 공동저장소 지원

- 운영 기관의 브라우저인증서 상호운용성 보장을 위해 공동저장소 사용(평상시 공동저장소에 보관, 이용자 전자서명 요청시 운영기관 저장소로 복사/이동 후 전자서명 지원)
- 금융결제원의 “브라우저인증서 공동저장소 개발자 매뉴얼”에 따라 공통 저장소 규격 개발 및 적용 솔루션 도입(금융결제원에서 배부 받은 테스트, 상용 API 키 설정을 통해 개발)

- 브라우저 인증서 운용

- 인증서 발급(재발급, 갱신 포함), 기존 장치에서 인증서 복사, 인증서 비밀번호 변경 시 운영기관 브라우저 저장소(이하, 운영기관 저장소)와 금융결제원 브라우저 저장소(이하, 공동저장소)에 동시에 인증서 저장 필수
- 인증서 삭제 시 운영기관 저장소와 공동저장소에서 동시 삭제
- 운영기관 저장소와 공동저장소에 동일한 인증서가 있는 경우 타임스탬프가 더 최근인 인증서 하나만 인증창에 표시
- 브라우저 공동저장소는 저장기능만 제공하고, 초기 이용 시 공동 저장소에 저장된 인증서를 운영기관 저장소로 복사하여 이용
- 금융결제원 전자인증부에서 발행한 “브라우저 인증서비스 가이드라인 2.0” 세부 내용에 맞춰 인증 창 페이지 도입(개발)

- 이용자의 브라우저 인증서 서비스 사용
  - 브라우저 인증서는 개인 신규 발행, 개인 기존 공인인증서 이동/복사 사용, 법인 기존 공인인증서 이동/복사 형태로 사용
  - 기존 공인인증서 사용 시 인증서가 저장된 PC 파일 경로를 찾아 공인인증서 파일(xxxx.der, xxxx.key) 두개를 동시에 선택한 후 인증창에 Drag&Drop으로 이동, 복사한 후 브라우저 인증서 사용 가능(기존 공인인증서 파일 경로 자동 탐색 및 브라우저인증서 전환을 지원하는 플러그인 이용자 선택 설치)
  - 비밀번호 입력 지원을 위한 가상키패드 제공

☀ 공인인증서 경로 예 : C:\Users\Wuser\AppData\Local\Low\WNPki\Wyessign\W  
C:\Program Files\WNPki\Wyessign\W

## 🔗 도입 시 유의사항

- 현재는 개인 고객만 사용 가능(향후 법인 지원 예정)
- HTML5를 지원하는 브라우저에서만 사용 가능

〈표 8〉 브라우저 인증서 지원 브라우저 현황

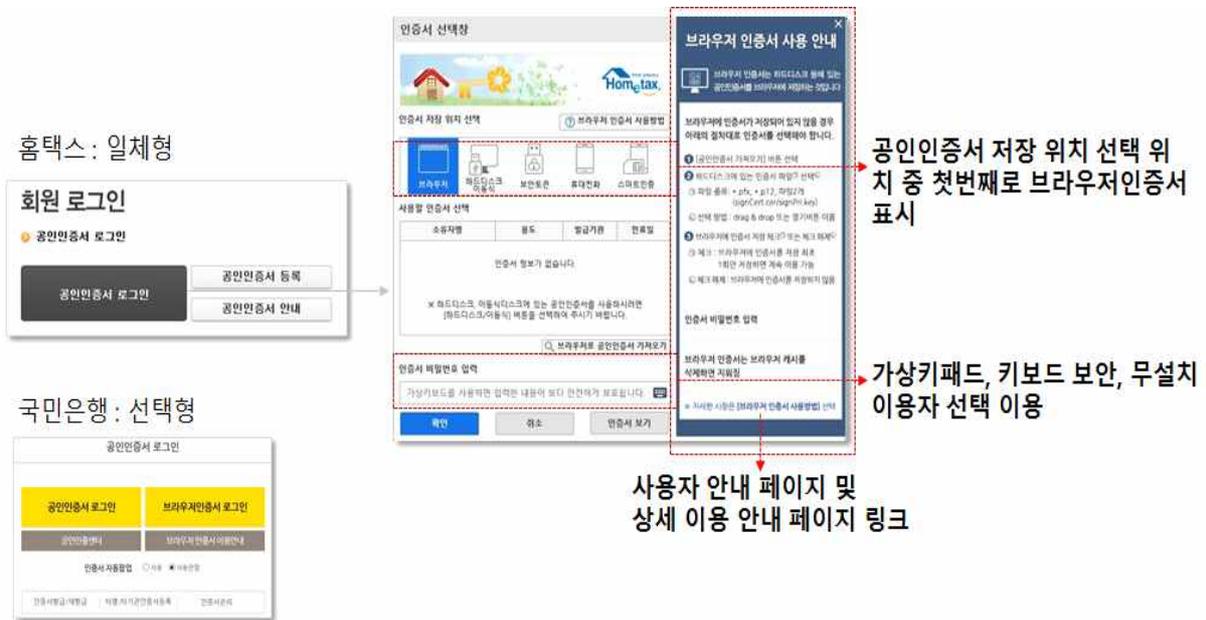
구분		이용환경
PC		MS IE 11 이상, Edge 12 이상, Chrome, Firefox, Safari, Opera
모바일	안드로이드	Android 5.0이상 기본 브라우저, Chrome
	iOS	iOS8.0 이상 Safari, Chrome

- 브라우저 인증서는 브라우저의 캐시(Cache) 데이터를 삭제하면 자동으로 인증서가 삭제, 이용자에게 캐시 삭제시 브라우저 인증서 삭제 안내 필요
- 브라우저 간 로컬 스토리지의 물리적 위치가 달라 브라우저 별로 공인인증서를 복사하고 이용해야 함(주 이용 브라우저에서 브라우저 인증서 사용 안내 및 웹사이트별 저장 필요)
- 금융결제원은 브라우저 인증서 보관(백업) 서비스를 통해 캐시 삭제 시 인증서 복구 서비스 지원 예정(2018.11 이후)
- 공인인증서 가져오기를 할 경우 이용자 플러그인 설치 옵션 선택 가능, 플러그인 선택 시 파일 가져오기 및 인증 파일 변환 기능 지원, 플러그인을 사용하지 않을 경우 이용자가 직접 인증서 선택 후 Drag&Drop으로 인증서 파일 가져오기 및 브라우저 공동저장소 저장

- 법인은 기존 발급 공인인증서에 한해 브라우저 인증서로 복사 사용 가능하나 직접 발급 방식은 향후 지원 예정
- 사설인증서 및 특수목적용 기관 인증서도 브라우저 인증서 기술 방식으로 지원 가능(브라우저 인증서 솔루션 공급사와 추가 개발 협의 필요)
- 주민번호를 수집할 수 없는 웹사이트의 경우, 본인확인을 위해서는 공인인증기관의 본인확인서비스(UCPID, Use of accredited Certificate for Personal Identification)사용 필요

### 🔗 적용 사례

- 국세청 홈택스, 국민은행 로그인, 신한은행 로그인, 대구은행 로그인, AIA생명보험 로그인에서 브라우저 인증서(복사사용방식) 및 가상키패드 도입 제공 중



| 그림 15 | 브라우저 인증서 서비스 제공 화면(출처 : 홈택스, 국민은행)

☀️ 공인인증서 로그인과 브라우저 인증서를 함께 표시하는 일체형과 공인인증서와 별도로 브라우저 인증서를 화면에 표시해서 이용자가 명시적으로 선택하는 선택형이 있음

## 4 전자결제

### 개요

전자결제는 세금 납부, 공과금, 범칙금, 과태료 납부, 환급 요청, 증명서 발급 수수료 결제 등을 위해 신용(체크)카드 결제나 계좌이체, 기타결제(휴대폰 소액, ARS 전화 등)등의 결제 방식 사용

플러그인 없는 전자결제는 2014년 9월, 금융위원회의 “전자상거래 결제 간편화 및 Active-X 해결 방안” 후속 조치를 통해 안전성과 무결성을 지원하는 전자결제 수단을 사용하는 경우 공인인증서 의무 사용 폐지

이에 따라 카드사나 전자금융업자(PG)들이 공인인증서 외에 대체 결제방식과 직접 카드정보를 수집, 저장하는 간편결제 서비스와 같은 플러그인 없는 결제 방식 제공

### 플러그인 사용 현황

전자결제를 위한 플러그인은 공인인증서 사용에 따른 전자결제창 보안, 카드(이체)결제모듈 플러그인 사용

#### ■ 전자결제창(결제창 보안, 키보드보안, 전송구간 암호화, PC방화벽)

- 전자 결제 서비스를 이용할 때에는 거래자의 신원확인, 결제 시점확인, 거래사실 부인 방지 등을 목적으로 공인인증 및 통합 보안 모듈(카드사 안심클릭, ISP인증 등) 사용

인증 방법	설명
안심 클릭 인증	카드 발행사와 카드 소유자간에 상호 알고 있는 정보를 토대로 안심클릭 인증정보를 생성하고 이용자가 등록된 올바른 인증정보를 제공할 수 있는지 여부로 본인확인
ISP 인증	카드 발행사와 카드 소유자간에 상호 알고 있는 정보를 토대로 ISP 인증정보를 생성하고 이용자가 등록된 올바른 ISP 인증정보에 근거하여 생성한 전자서명(Digital Signature)을 서버에서 검증하여 카드 소유자 본인확인

## ■ 카드(계좌이체)결제모듈

- 카드사 전자결제창과 PG사간 전송구간 암호화, 키보드보안, 다양한 전자결제 (PG사 계좌이체, 가상계좌, 에스크로, 휴대폰 결제)지원 프로그램

### 대체 방안

## ■ 신용카드 수기특약(키인 방식)

### 🔗 기술 개요

기존 카드 결제 화면은 카드사가 직접 관리하고 있는 영역으로 플러그인 제거를 위해서는 아래와 같은 플러그인 없는 결제 방식 도입 필요

- 카드 결제 화면(시스템)을 운영기관이 운영할 수 있는 키인 방식 수기결제 도입 (카드사와 수기특약 가맹점 계약 및 수기결제 PG와 운영기관 간 삼자 계약진행)
- 간편수기결제 PG와 가맹점 계약 후 간편수기결제 PG와 결제모듈(API) 연동

이를 통해 신용카드 번호, 유효기간, 카드비밀번호(두 자리), 식별 번호 등을 버튼 입력(키인 방식)으로 입력받아 카드결제를 실행

키인 방식 수기결제 도입 시 별도 플러그인 없이 카드 결제를 할 수 있는 장점이 있으나, 카드 정보 및 개인 정보를 서비스 운영기관이 저장, 관리함으로써 보안 관리 및 PG와 전송구간 암호화 연동 지원 필요

🔗 카드 데이터 : 신용카드 번호, 유효기간, 카드 비밀번호 앞 2자리

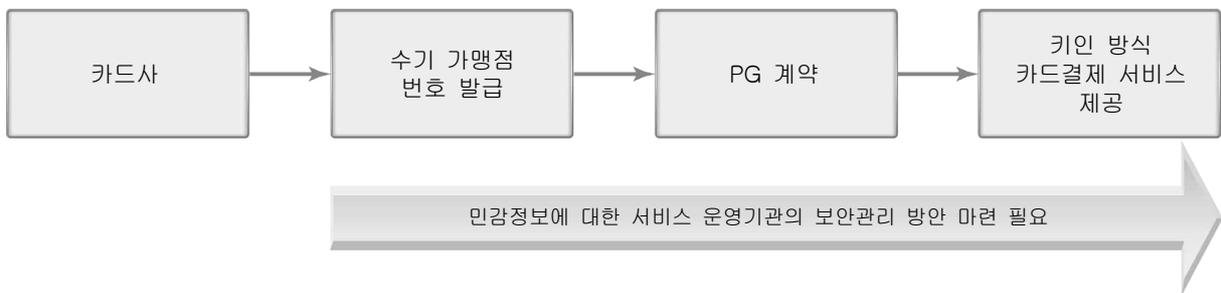
🔗 개인 정보 : 성명, 회원 아이디, 주민번호 앞자리/법인 번호

이외에 간편수기결제 PG 계약을 통해 서비스를 제공받을 수 있음. 이 경우 가맹 계약 외에도 월 거래 한도와 연동한 보증보험 가입 필요

### 🔗 적용 방법

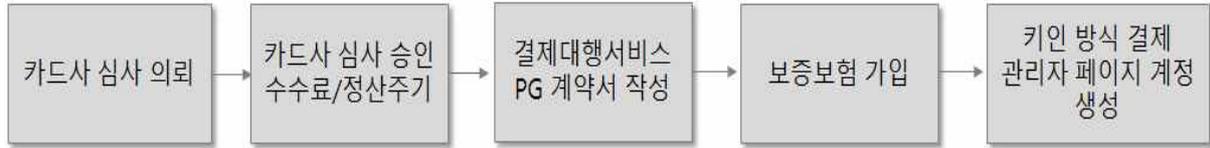
- 수기특약 카드결제(키인 방식) 서비스 개발
  - 카드사에 운영기관 정보 제공(카드사 심사의뢰)
  - 각 카드사의 심사 승인 획득 및 수기특약 가맹점 계약(수수료, 정산주기 확인)

- 수기 결제 PG와 결제 대행 서비스 계약 진행
- 수기 결제 PG 계약 후 결제 연동 규격서 수령
- 키인 방식 결제 페이지와 PG 연동 인터페이스에 보안 안전관리 방안 조치(수기결제 PG와 협의 구축)
- 수기특약 서버 모듈 설치(Socket 방식 or API 방식으로 수기결제 PG 연동)
- 안전 카드 결제를 위한 추가 개발 사항 확인(사고카드 조회, 이상 거래 탐지, 응답세션 관리 등)
- 수기특약 서버 모듈 설치(소켓 방식 or API 방식으로 PG 연동)
- 카드 정보 입력 페이지의 SSL 적용 및 데이터 암호화
- 카드데이터, 개인 민감정보 암호화 모듈 설치(연동, 저장, 관리)
- 키인 방식의 결제 화면 개발 및 PG 연동 테스트 진행



| 그림 16 | 카드사 수기특약(키인 방식) 가맹 프로세스

- 간편수기결제(키인 방식) PG 연동
  - 간편수기결제 업체 선택, 운영기관 정보 카드사 심사 의뢰
  - 카드사 심사 승인 획득 및 수수료, 정산주기 확정
  - 결제 대행 서비스(간편수기결제 PG)와 계약서 작성 및 전달
  - 일/월 결제 거래 한도에 따른 보증보험 가입
  - 수기특약 서버 모듈 설치(소켓 방식 or API 방식으로 PG 연동)
  - 수기 결제에 필요한 보안 조치를 간편결제 PG사가 담당하고, 웹 링크 방식으로 PG사가 제공하는 결제 사이트에서 수기 입력 방식으로 카드 결제
  - 운영기관이 활용할 수 있는 관리자 페이지 계정 생성 및 부여
  - 테스트 및 신용카드 결제 서비스 제공



| 그림 17 | 간편수기결제 가맹 프로세스

### 🔗 도입 시 유의사항

- 카드사와 키인 방식 수기 특약 계약 조건 확인 필요(보안 조치, 월간 한도, 보증 보험 가입 등)
- PG 계약 시 수기 특약의 경우 카드정보 및 민감정보에 대한 서비스 운영기관의 보안 관리 방안 마련 필요(침입탐지시스템, DB암호화 및 전송구간암호화 등)
- 간편수기결제 PG 계약과 동시에 일반 PG 계약 필수, 삼자(웹사이트 운영기관, PG사, 신용카드사) 계약 후 카드사 심사 청구 진행

### 🔗 적용 사례

- 코레일 열차 예약/발급 서비스, CGV 좌석 예약 서비스

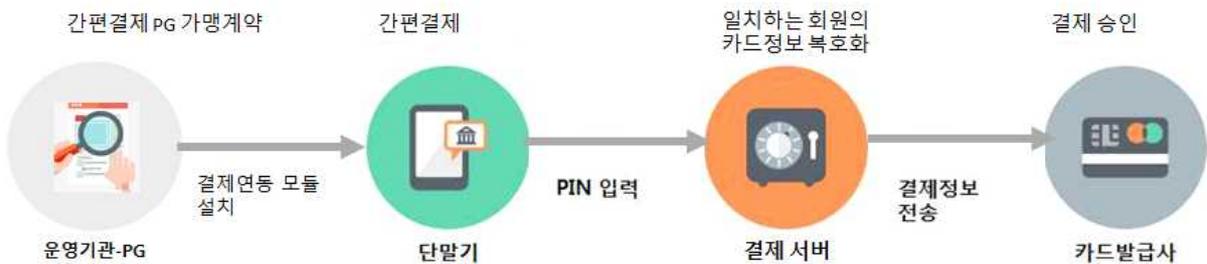
신용카드	계좌이체	포인트
카드종류	<input checked="" type="radio"/> 개인카드 <input type="radio"/> 법인카드	
신용카드 번호	[ ] - [ ] - [ ] - [ ]	
유효기간	[ 선택 ▼ ] 월 [ 선택 ▼ ] 년	
할부개월	[ 일시불 ▼ ]	
신용카드 비밀번호	[ ] ** (앞2자리)	
인증번호	[ ] (주민번호 앞 6자리)	
<input type="checkbox"/> KTX마일리지(-)	0 [ ] 원	[ 조회 ]
<input type="checkbox"/> 위비풀머니(모아)(-)	0 [ ] 원	[ 조회 ]
<input type="checkbox"/> 씨티포인트(-)	0 [ ] 원	[ 조회 ]
<input type="checkbox"/> OK CASHBAG 이벤트 ▶	0 [ ] 원	[ 조회 ] [ 자세히... ]
<input type="button" value="발권하기"/> <input type="button" value="전달하기"/> <input type="button" value="장바구니"/> <input type="button" value="예약취소"/>		

| 그림 18 | 카드결제 수기특약에 따른 결제 서비스화면(출처 : KTX)

## ■ 간편카드결제

### 🔗 기술 개요

간편카드결제 PG 연동을 통해 ARS나 SMS등을 통해 본인확인 후 이용자가 등록한 카드 정보와 6자리 PIN번호를 통해 간편카드결제 PG에 저장된 카드 정보를 복호화하고, 이를 데이터 서버로 전송하여 결제 정보를 결합시킨 후 결제 정보를 신용카드사로 전송하는 방식으로 카드 결제 서비스 제공



| 그림 19 | 간편카드결제 방식 예시

### 🔗 적용 방법

기존 계약 PG사에 플러그인 무설치 간편 카드, 계좌이체 결제 지원 여부 확인  
기존 PG가 간편카드결제/간편계좌이체를 지원하지 않을 경우 계약 종료일 및 계약 옵션 확인 후 신규 간편결제(간편계좌이체)PG 도입 진행(가맹 계약, 가맹점 코드, 수수료, 도입 일정, 도입 시 추가 개발 내용 확인)

- 간편카드결제 가맹 계약
  - 웹 방식으로 카드 결제를 지원 하는 PG사 선택 후 가맹점 계약 진행
  - 운영기관 일/월간 결제 금액에 따라 보증보험 가입 및 보증 금액 확인
- 간편카드결제PG 연동
  - 간편결제 코드 발급, 수령 및 PG 결제시스템 연동(페이지 링크, API 방식)
  - 페이지 링크 방식은 URL 호출을 통해 결제 PG사의 결제창을 호출하는 방식과, PG에서 전달받은 자바스크립트 라이브러리를 통해 API 형태의 결제 정보를 통해 결제 서비스 제공
  - 정상 결제 여부는 PG사에서 전달한 메시지 값을 통해 확인(중복 여부, 사고 카드 여부, PIN번호 오류, 부정거래 등)
  - 간편결제 연동 테스트 및 PG 검수 및 신용카드사 심사

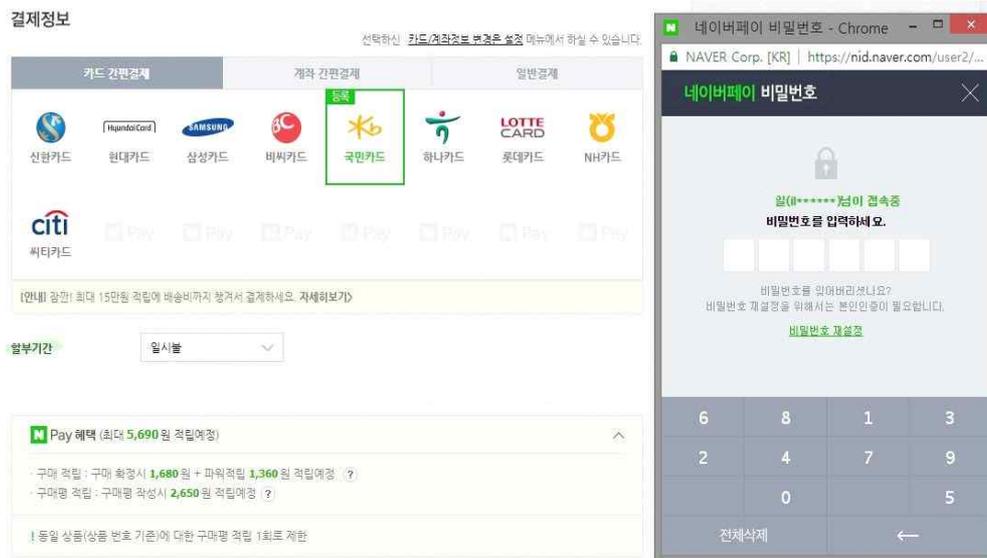
- 정상 결제 동작 확인
  - 간편결제 통계, 정산 정상 여부 확인
  - 간편카드결제 서비스 오픈

## 🔗 도입 시 유의사항

- 간편결제 PG 선택 시 별도 플러그인 설치없이 웹만으로 신용, 카드 결제 서비스 제공 사업자 선택(본인 확인 시 SMS나 ARS 활용 가능)
- 모바일 앱 설치를 통한 간편결제 방식은 권장하지 않음
- 대부분 웹 결제를 제공하는 간편결제 PG는 모바일 웹에서도 간편결제 지원(웹, 모바일 웹 동시 간편결제 제공 가능)
- 간편결제 PG는 1회/1일 결제 한도 있음(한도 조정 가능)

## 🔗 적용 사례

- 대부분의 온라인 판매 사이트에서 사용 중

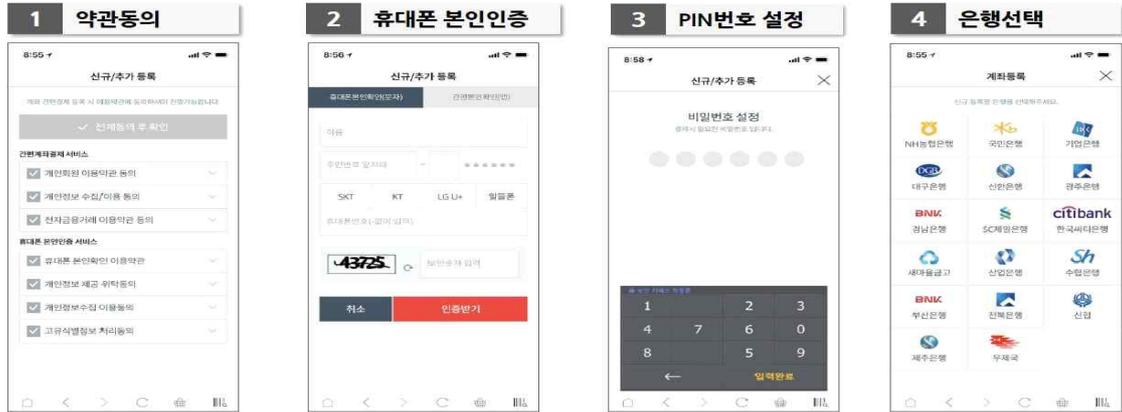


| 그림 20 | 간편카드결제 예시(출처 : 네이버페이)

## ■ 계좌간편결제

### 🔗 기술 개요

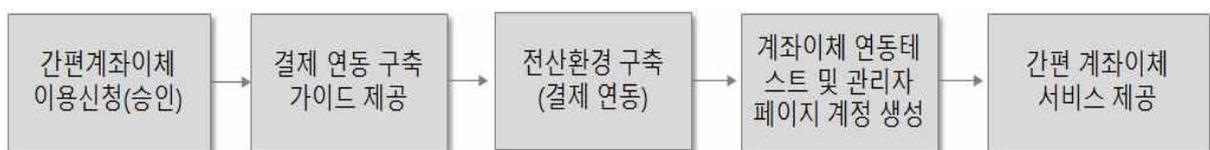
간편결제 PG 중 웹 방식으로 본인계좌 이체 결제를 제공하는 계좌간편결제 PG와 가맹점 계약을 통해 이용자 통장 계좌의 현금 이체 서비스 지원



| 그림 21 | 계좌간편결제 이용 절차(웹, 모바일 웹 지원)

### 🔗 적용 방법

- 계좌간편결제(키인 방식) PG 연동
  - 계좌간편결제 PG 업체 선택
  - PG사와 수수료, 정산주기 확정
  - 계좌이체 결제 대행 서비스 계약서 작성 및 전달
  - 일/월 결제 거래 한도에 따른 보증보험 가입
  - 계좌간편결제 서버 모듈 설치(소켓 방식 or API 방식으로 PG 연동)
  - 간편계좌결제 PG 연동 인터페이스 개발
  - 간편계좌결제 입력, 연동 페이지 개발(SSL 적용)
  - 간편계좌결제 연동 테스트 서비스 제공
  - 운영기관이 활용할 수 있는 관리자 페이지 계정 생성 및 부여



| 그림 22 | 계좌간편결제 가맹 프로세스

## 🔗 도입 시 유의사항

- 계좌 이체시 본인확인 및 본인 계좌 확인을 위해 휴대폰 SMS, ARS 인증 제공
- 이용자 본인 계좌 확인을 위해 1원 입금 검증 적용(PG사에서 검증)
- 1일, 1회 계좌이체 금액이 높은 운영기관은 결제 금액 한도에 대해 PG와 협의
- 계좌간편결제 PG에 따라 지원 가능 은행/증권사 리스트 확인 필요
- 은행 및 증권사 레거시 시스템 특성 상 일거래 결산 문제로 일 30분 정도 이체 서비스 중단(23:50~00:20)
- 네이버페이의 경우 자사 ID(계정) 보유 이용자에 한해 계좌이체 가능
- 계약 조건에 따라 계좌이체 수수료와 최소 계좌 이체금액 있음

## 🔗 적용 사례

- 네이버페이, 위메프/쿠팡/티몬, 스마일페이, 세틀뱅크 계좌간편결제

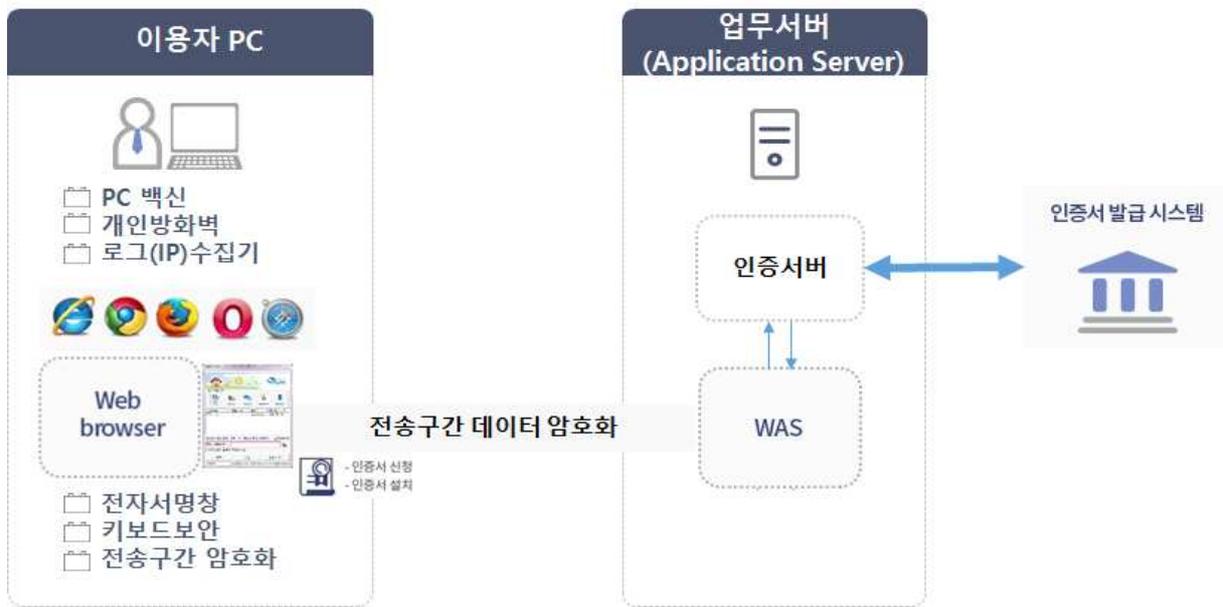


| 그림 23 | 계좌간편결제 방식 예시(출처 : 네이버페이)

## 5 PC 및 공인인증서 보안

### 개요

PC 및 공인인증서 보안은 공공 웹사이트 이용자의 PC 보호 위한 PC 백신, 개인방화벽(로그수집기 포함) 플러그인 사용과 본인확인 및 전자서명의 안전한 이용을 위한 공인인증서 전자서명창, 키보드보안, 전송구간 암호화 플러그인 사용



| 그림 24 | PC 및 공인인증서 보안 플러그인 유형

### 플러그인 사용 현황

이용자 PC 및 웹서비스 이용 시 보안 침해 방지를 위해 PC 백신, 개인방화벽, 키보드보안, 전송구간 암호화, 전자서명창 보안 플러그인 사용

#### ■ PC백신 및 개인방화벽(로그수집기)

- 본인확인 및 전자 결제, 전자문서 전자 서명 시 이용자 PC 및 실시간 변경되는 주요 입력 정보(OTP, 보안카드 번호)를 보호하기 위해 실시간 악성코드 탐지, 원격 침해 프로그램 탐지 및 차단, 피싱/파밍에서 이용자 보호 및 네트워크 환경에서 E2E 암호화를 위해 사용
- 공공조달에서 동일 IP(Internet Protocol) 중복, 부정 입찰 여부 확인을 위해 맥어드레스(물리적 주소) 및 IP 정보 수집을 위한 로그수집기 사용

## ■ 키보드 보안

- 이용자가 입력하는 개인정보, 금융 정보 등의 기밀 데이터의 입력 값을 다양한 해킹 공격이나 기밀성 보장을 위해 사용하며, 물리적 키보드 데이터를 시스템 커널(Kernel)의 키로거 접근 차단 및 백도어 또는 해킹툴에 의한 키 입력 가로채기 방지, 실시간 키보드 입력 정보를 암호화 후 서버에 데이터 전달 기능 제공

 키보드보안 플러그인 사용 시 불편사항

**(윈도우)** 커널 접근시 제품 충돌로 인해 OS가 리부팅 되거나, 사이트 별 중복 설치 및 메모리 과다 점유 문제

**(리눅스)** 키보드 보안을 설치할 경우 Root 계정 권한을 요구 및 시스템 전체의 보안성을 위협하는 결과 초래

## ■ 전송구간 암호화

- PC 웹브라우저에서 서버, 또는 서버에서 서버로 전송하는 데이터를 안전하게 암호화 하는 프로그램

## ■ 전자서명창 보안

- 공인인증서 유효성 확인 및 비밀번호 입력 화면보호, 인증서 발급, 갱신, 폐기 관리 기능을 지원하는 프로그램

## 대체 방안

## ■ PC 백신, 개인방화벽, 키보드보안 플러그인 이용자 선택 설치

### 기술 개요

이용자 PC의 악성프로그램(스파이웨어, 악성코드, 랜섬웨어 등)등을 검출하거나 치료하는 PC 백신이나 외부 침입자(해커)로부터 이용자 PC를 보호하는 개인방화벽의 경우 이용자가 설치한 상용(무료) 백신에 주요 기능이 탑재되어 운영기관에서 보안 플러그인을 별도 배포할 경우 이용자 PC에 중복 설치됨

PC 백신, 개인방화벽 기능은 Windows7 이상에 기본 탑재된 윈도우 Defender나 Mac OS 게이트 키퍼, 상용(무료) 안티바이러스 제품 사용만으로도 이용자 PC 보안 및 악성 프로그램 자동진단 및 차단 가능

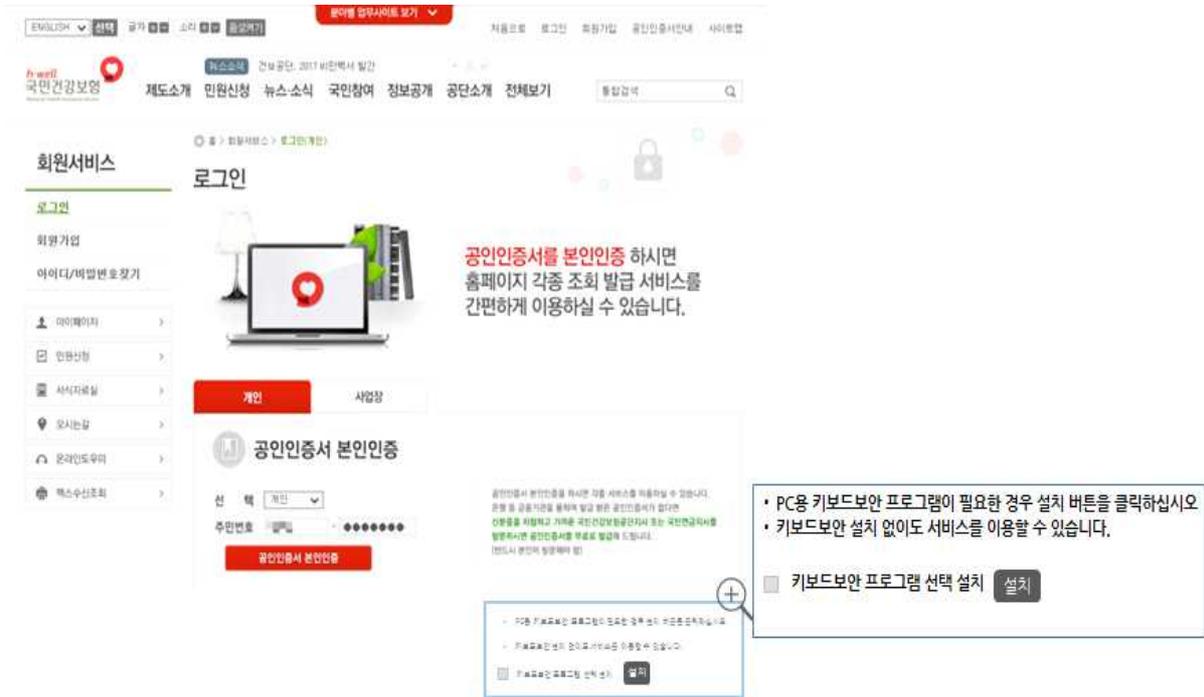
이용자 PC나 브라우저(웹 페이지) 입력 값의 키로깅 방지를 위해 설치하는 키보드보안은 사용 방식에 따라 이용자 선택 설치 또는 웹표준 기반 가상키패드로 구분해서 사용

## 🔗 적용 방법

- 본인확인 및 본인인증(공인인증서 로그인), 전자문서의 전자서명에 공인인증서를 사용할 경우 이용자에게 상용(무료) PC 백신(대부분의 상용 PC에 개인방화벽 기능 내장되어 있음) 사용을 권장하고, 이용자가 개인방화벽, 키보드보안 플러그인 설치를 희망하는 경우에만 이용자 선택 설치
- 브라우저 인증서 사용 시 가상키패드 사용 권장(이용자 선택에 따라 키보드보안 플러그인 설치 가능)
- 이용자 선택 플러그인 설치 화면은 이용자가 명시적으로 설치에 동의하기 전까지 설치 금지
- 설치할 플러그인 이용목적 설명 제공 및 이용자가 선택할 수 있는 명시적인 설명 제공
- 팝업이나 다이얼로그 방식이 아닌 체크 박스 선택 화면 방식 제공
- 이용자에게 설치를 유도하거나 설치하지 않을 경우 이용 불편을 강조하는 화면 레이아웃 배제

## 🔗 도입 시 유의사항

- 기존 공인인증서를 통한 본인확인, 전자문서의 전자서명 시 비밀번호 입력의 경우 다른 보안 모듈(전자서명창, 전송구간암호화) 연동 시 복호화 되는 보안취약점으로 인해 완벽한 보안성을 보장하기 어렵다고 알려져 있음
- 웹표준 기반 가상키패드는 이용자가 입력한 값의 브라우저(웹페이지)-서버 간 E2E 보안을 지원함



| 그림 25 | 플러그인 사용 안내 및 설치 등의 화면 가상 예시

## ■ 웹표준 기반 가상키패드

### 🔗 기술 개요

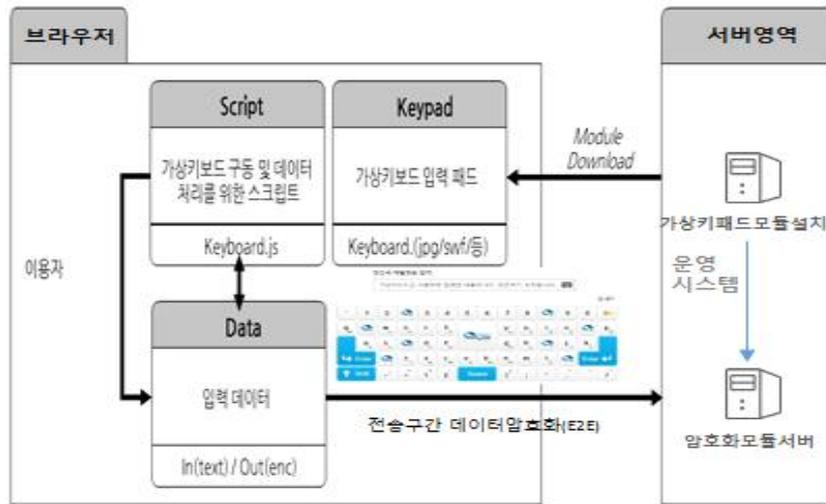
가상키패드는 숫자 또는 문자가 표시된 키패드 이미지와 이를 처리하기 위한 스크립트 파일을 서버에서 이용자 웹페이지로 전송하고, 이용자가 마우스를 이용해 입력한 정보를 암호화하여 서버 전송

가상키패드는 공인/브라우저인증서의 비밀번호 입력 외에도 주요 개인정보 입력 등에도 사용할 수 있으며, 운영기관의 서비스 서버에 가상키패드 모듈 설치를 통해 플러그인 설치없이 웹표준 방식의 가상키패드 제공

### 🔗 적용 방법

- 운영기관 서버에 가상키패드 모듈 및 암호화 모듈 설치 및 모듈 간 상호 연동
- 인증서 선택창 팝업(입력창)에 서버에서 생성한 가상키보드 입력 패드(암호화된 좌표) 적용
- 암호화 및 데이터 처리 스크립트, 가상키패드 이미지 연동
- 가상키보드 입력 데이터 전송구간 데이터 암호화 적용 및 암호화 모듈 서버 전송 확인

- 설치-데이터 전송까지 보안 기능 정상 동작 여부 확인(키로깅방지, 랜덤키패드, 세션관리, 입력좌표변조, 멀티커서 등)



| 그림 26 | PC 가상키패드 주요 흐름

### ☞ 도입 시 유의사항

- 가상키패드 적용시 전송 구간의 보안 요구사항(E2E 보안, 키로깅방지, 랜덤키패드, 세션 관리, 입력좌표변조, 멀티커서, 자바스크립트 난독화 등)을 준수한 안전한 가상키패드 솔루션을 도입

### ☞ 적용 사례

- 홈택스 브라우저 인증서 가상키패드, 국민은행, 신한은행 가상키패드



| 그림 27 | 가상키보드 적용 사례(출처 : 홈택스)

## ■ 전송구간 암호화(SSL)

### 🔗 기술 개요

전송구간 암호화는 PC의 웹브라우저 서버로 전송하는 중요 데이터를 검증된 암호화 알고리즘을 통해 암호·복호화하여, 비인가자나 악의적인 이용자가 전송 데이터 패킷을 가로채더라도 쉽게 데이터 내용을 파악하지 못하도록 함

이를 통해 공인인증서 전자서명창과 인증 서버 간의 통신이나 웹서버와 웹서버간의 통신구간에 전자금융 정보나 개인정보 등 민감 정보(예: 신용카드 번호, 주민등록번호, 이용자 이름, 전화번호, 비밀번호, OTP번호 등) 데이터가 전송되는 과정에서 공격자에게 데이터가 노출되는 것을 방지하거나, 악의적인 데이터 변경을 방지하기 위해 사용

전송구간 암호화는 기본적으로 플러그인 설치가 필요 없는 SSL(Secure Socket Layer)을 사용하여 기밀성과 데이터 무결성을 보장하고 상호 식별 및 인증 제공 가능

HTML5 표준으로 WebCrypto API 및 국산 블록암호 알고리즘과 인증 등에 사용되는 암호기술 및 웹서비스 보호 방법에 대해서는 한국인터넷진흥원의 “HTML5 암호기술 이용 안내서(2015)”을 참조하여 구현

### 💡 참고자료

- 행정안전부 “홈페이지 SW(웹) 개발보안 가이드”(2012)
- HTML5융합기술포럼 “W3C의 웹보안 동향과 HTTPS 구축 지침”(2017)
- OWASP(The Open Web Application Security Project) “OWASP Top 10 - 2017”
- 보안서버 구축 가이드(과학기술정보통신부, 2013)

### 🔗 적용 방법

- SSL 보안서버 인증서 발급 기관을 통해 인증서 유형별 발급 절차에 따라 발급 및 웹서버 종류별 SSL 보안서버 구축
  - IIS 서버, Apache 서버 등 웹서버 기종에 따른 설치 과정 확인
  - SSL 모듈 서버 설치 및 환경파일 설정
  - 서버 재구동 및 SSL 정상 동작 여부 확인

- 안전한 전송구간 암호화 및 보안 설정을 위해 G-SSL 인증서나 SSL 인증서를 웹서버에 설치
- 웹사이트의 신원을 인증(해당 사이트가 위조 사이트가 아님을 보장)
- 전송되는 웹 구간 데이터를 SSL 인증서를 통해 암호화, 이때 사이트 규모 및 SSL 적용 범위, 사이트 보안 등급에 따라 SSL 인증 시스템(인증서, 서버 에이전트) 선별 도입
- 하위 도메인 수에 따른 SSL 인증서 유형
  - 싱글 : 완전한 자격을 갖춘 도메인 네임이나 하위도메인 네임 한 개의 보안 지원
  - 와일드카드 : 한 개의 도메인 네임과 무한대의 소속 하위 도메인을 보안 처리
  - 멀티 도메인 : 복수의 도메인 네임을 보안 처리
- 웹사이트 인증 도입 수준
  - 도메인 인증 : 기본 암호와 도메인 네임 등록 소유권의 인증(가장 단시간에 발급 가능)
  - 조직 인증 : 기본 암호와 도메인 네임 등록 소유권의 인증, 소유주의 특정 세부내역(예: 이름 및 주소) 인증(며칠 후에 발급)
  - 확장 인증 (EV) - 인증서를 발급하기 전에 철저한 조사를 수행 후 최고 수준의 보안 등급을 제공. 도메인 네임 등록 소유권 및 법인 인증에 추가하여, 해당 법인의 법적, 물리적 그리고 운영상의 존재를 인증(몇 주 후에 수령)

SSL 인증서는 인증서를 요청하는 법인의 신원과 적법성을 확인하도록 의뢰를 받는 조직인 Certificate Authorities (CAS)가 발급하며, 이를 웹서버에 설치하여 운영
- 인증서 정상 동작 확인
  - URL 옆의 자물쇠(열쇠)표시 또는 http 대신 https URL 접두사
  - 트러스트 쉘 또는 녹색 주소창(EV SSL 인증서 발급 시)
  - G-SSL 서버 인증서는 IE8~11에서 인증서 발급정보 확인, 크롬 브라우저에서 인증서 표시 발급기관(CA131100001), 파이어폭스는 “안전하지 않는 연결”, 사파리는 “확인할 수 없음”으로 표시되거나 보안 예외 추가를 통해 사이트 조회 가능(인증서 정상 동작)



| 그림 1 | G-SSL 적용 인증서 브라우저 표시 확인(출처 : 경찰청)

## 🔗 도입 시 유의사항

- 보안 서버 구축 안내서(한국인터넷진흥원, 2009)의 “Ⅲ. SSL 방식 보안서버 구축하기”를 참고하여 SSL 최적화 설정
- 안전한 TLS(Transport Layer Security) 파라미터 설정
- SSL 적용시 속도 저하가 발생할 경우 SSL에 대한 올바른 설정이나, 일부 웹페이지에서만 선택적으로 SSL을 적용해서 해결 가능
- 키교환(ECDHE, DHE), 서버 인증(authentication), 암호(AES 128), 모드(GCM/CCM), 무결성 보장(SHA256 이상) 설정 확인
- Cipher Suite는 SSL 또는 TLS 연결이 사용하는 여러 프로토콜과 암호화 알고리즘, 인증서 검증 방식을 설정해 놓은 것으로 브라우저를 구분해서 최적화된 조합 선택
- 브라우저 개발사가 인정한 안전한 SSL 인증서 사용 및 전자정부 서비스 호환성 준수지침에 따라 크로스 브라우저에서 인증서 정상 동작 여부 테스트
- SSL 도입 시 성능향상을 위해 웹서버 설정으로 압축 데이터 연동 방식과 성능저하의 원인인 RSA연산과 AES 연산 성능 향상을 위한 서버 연산가속기를 사용하는 방법으로 가속 대상은 인증서를 사용 부분, 키교환을 하는 부분, 데이터를 주고받는 부분에 적용
- G-SSL(Government Secure Socket Layer) 인증서를 도입할 경우 행정전자서명 인증관리센터(<https://gcert.gpki.go.kr>)에서 제공하는 “전자정부 웹서비스 인증서(G-SSL) 구축가이드”의 웹트러스트 인증 갱신 및 G-SSL 인증서 멀티브라우저 등록 규격에 따라 변경 구축
- G-SSL 인증서 종류 및 용도 선택 시 “기관용“, ”SSL용“ 인증서 선택(유효기간 2년 3개월)
- G-SSL 인증서 발급절차는 “한국지역정보개발원 부서명추가필요“에 문의 후 발급 처리

## 🔗 적용 사례

- 국세청 홈택스 홈페이지, 국민건강보험 홈페이지, 과학기술정보통신부 홈페이지, 이니시스 웹표준 결제창



| 그림 28 | 크롬 웹 주소창 SSL 인증서 적용화면(출처 : 홈택스)

### ■ 브라우저 인증서

본문 중 “3. 전자서명 중 브라우저 인증서” 내용 참조

## 6 전자문서 조회 및 보안

### 개요

민원문서 열람, 교부, 신청을 위한 문서 폼 생성, 시점확인, 조회화면보호 기능을 제공하기 위해 플러그인 사용

### 플러그인 사용 현황

#### ■ 전자문서 조회(뷰어)

- 다양한 리소스(DB, CSV, XML, JSON, SAP, HWP 등)의 PDF 전환 및 문서 뷰어 기능 제공 프로그램(서버 부하 경감을 위해 클라이언트 서식생성 방식 지원)

#### ■ 조회화면 보호

- 웹페이지 및 전자문서 조회화면 무단 캡처(복제) 방지, 소스 유출 차단을 위한 프로그램

#### ■ 시점 확인(타임스탬프)

- 전자문서 생성시점(Time Stamping Authority)의 법률적 증명과 위·변조 방지를 위해 특정 시점에 존재하였으며, 그 이후 변경되지 않음을 증명해 주는 프로그램
- 시점 확인의 안전성을 보장받기 위해서는 PKI 기반 전자서명과 타임스탬프 및 장기 검증 등의 아래 5가지 핵심 요소 지원하며, 이용자 PC의 무결성, 적시성 상호 검증 및 TSA 검증을 위해 플러그인 사용

〈표 9〉 전자문서 시점 확인 기능 및 현황

구분	기능	현황
전자문서 시점확인	TSA 인증	서버에서 인증 지원(현재도 서버에서 하는 곳 많음)
	TSA 검증	사용자가 문서의 위변조 검증을 원할 경우, 인터넷발급문서 진위확인 서비스에 관련 기능 개발(현재는 PC에서 검증 할 수 있는 모듈 다운로드)

### ■ 웹표준 조희화면 보호

#### 🔗 기술 개요

웹 페이지에 자바스크립트 코드를 통해 특정 키 이벤트, 마우스 이벤트 제어를 통해 웹페이지 및 전자문서 조희화면 무단 캡처(복제) 방지 지원

웹표준 조희화면 보호는 브라우저 메뉴 제어나 개발자 도구 열람 방지 등을 지원할 수 없어, 자바스크립트 난독화, 클라이언트 서버 유효성 검증을 통해 클라이언트 소스 변경에 대한 대응이 필요함

#### 🔗 적용 방법

조희화면 보호 기능에 대한 효용성과 필요성을 재검토하여 반드시 필요한 경우만 적용

#### ○ 웹표준 조희화면 보호 솔루션 도입

- 기존 플러그인 방식의 조희화면 보호 솔루션을 웹표준으로 구현된 조희화면 보호 솔루션으로 전환
- 도입 시 웹표준으로 지원 불가 내용 확인(브라우저 메뉴 제어, 프린터 제어, 개발자도구 이용 방지 등)

#### ○ 웹표준 조희화면 보호 개발

- 웹표준 조희화면 보호나 특정 기능 제어를 위해 자바스크립트를 통해 마우스 이벤트 제어 및 특정 기능을 제어
- 조희화면 기능 개발 소스를 보호하기 위해 소스(동적)난독화 및 동적 로딩 등의 기능을 통해 자바스크립트 소스를 보호 지원
- 자바스크립트 키보드, 마우스 이벤트 제어 및 CSS 설정을 통해 조희화면 보호(웹 DRM) 기능을 직접 구현하거나 웹표준 웹 DRM 솔루션 도입을 통한 조희보호화면 지원
- 자바스크립트(클라이언트)만의 유효성 검사는 악의적인 클라이언트 소스 변경을 통해 위조(회피)할 수 있어, 중요한 입력 데이터(회원 정보, 결제 정보, 실행 결과값 등)는 서버에서 검증코드 작성 후 입력 값을 검증하는 방식으로 구현

〈표 10〉 웹 DRM 웹표준 전환 방안

웹표준 전환 주요 기능	지원 브라우저	개선 방안
마우스 제어 (우클릭, Drag&Drop)	전체	자바스크립트 이벤트 제어 코드(소스난독화 처리)
키보드 제어 (Ctrl+PrtSc, Ctrl+P, Ctrl+A, Ctrl+V, Ctrl+X)	전체	자바스크립트 이벤트 제어 코드 작성(소스난독화 처리)
캡처 방지 (우클릭, Drag&Drop)	전체 (화이트, 문구 처리)	자바스크립트 이벤트 제어 코드(소스난독화 처리)
소스보기 제어 (우클릭)	전체	자바스크립트 이벤트 제어 코드(소스난독화 처리)
프린터 출력 제어	전체	Prt 키만 제어 가능
클립보드 사용시 특정 단어 표시	전체	자바스크립트 이벤트 제어 코드(소스난독화 처리)
개발자도구 보기 제어	크롬만 가능	자바스크립트 이벤트 제어 코드(소스난독화 처리) 클라이언트 자바스크립트, 서버 유효성 검사
소스 보기	전체	소스보기 화면에 마우스 제어 우클릭 이벤트 제어를 통한 화면조회보호 클라이언트 자바스크립트, 서버 유효성 검사
브라우저 메뉴 제어	전체 불가	클라이언트 자바스크립트, 서버 유효성 검사

● 웹표준 조회화면 보호 기능

- ① 마우스 키보드 제어(메뉴, 드래그, 선택복사 금지)
- ② 키보드 키 값 확인
- ③ 새로고침(F5), 전체창(F11) 막기
- ④ 상태바의 링크 주소 감추기
- ⑤ 클립보드 사용시 특정 단어 표시
- ⑥ 동영상 마우스 이벤트 막기
- ⑦ 프레임 소스보기 막기
- ⑧ 프린터 스크린 키 막기

● 자바스크립트 코드 난독화를 통해 코드 최소 보안 준수

● 조회 화면 보호 수준에 따라 자바스크립트로 특정 기능 추가 구현

● 자바스크립트 소스코드에 대한 위변조를 방지하기 위해 서버, 클라이언트 유효성 검증 기능 추가

### ① 마우스 오른쪽 키, 드래그, 선택복사 금지하기

```
<if (navigator.appName == "Netscape"){
  document.captureEvents(Event.MOUSEDOWN)
  document.onmousedown = checkClick
  function checkClick(event) {
    if (event.which != 1) {
      alert('마우스 오른쪽 버튼이 금지되었습니다')
      return false
    }
  }
}
```

### ② 키보드 키 값 확인(키값 확인 코드)

```
<script>
function keyDown(){
  var keycode = event.keyCode;
  var realkey = String.fromCharCode(event.keyCode);
  alert("keycode: " + keycode + "\nrealkey: " + realkey);
}
document.onkeydown = keyDown
</script>
```

### ③ 새로고침(F5), 전체창(F11) 막기

```
function processKey() {
  if( (event.ctrlKey == true && (event.keyCode == 78 || event.keyCode == 82)) ||
    (event.keyCode >= 112 && event.keyCode <= 123) || event.keyCode == 8) {
    event.keyCode = 0;
    event.cancelBubble = true;
    event.returnValue = false;
  }
}
document.onkeydown = processKey;
```

### ④ 상태바의 링크 주소 감추기

```
<script language=JavaScript>
setInterval("x()",1);
function x(){
  window.status="XXX"
}
</script>
```

⑤ 클립보드 사용시 특정 단어 표시

```
<script type="text/javascript">
  function OnCopy () {
    if (window.clipboardData) {
      window.clipboardData.setData ("Text", "열람정보 무단 복사금지");
    }
    return false; // cancels the default copy operation
  }
</script>
<body oncopy="return OnCopy ()">
```

⑥ 동영상 마우스 이벤트 막기

```
<param name="EnableContextMenu" value="false">
```

⑦ 프레임 소스보기 막기

```
<script language="JavaScript">
if(parent.frames.length <= 0) { top.location.href=url; }
</script>
```

⑧ 프린터 스크린 키 막기

```
function checkKeyPressed(e) {
  if (e.keyCode == "44") {
    alert("The print screen button was pressed.");
  }
}
window.addEventListener("keyup", checkKeyPressed, false);
```

○ 스크린 워터마크

증명서 조회화면에 로그인 사용자 정보를 워터마크 형태로 표현해 캡처 및 사진 촬영 시 유출 경로와 유출자를 확인



| 그림 29 | 스크린 워터마크 적용 전후

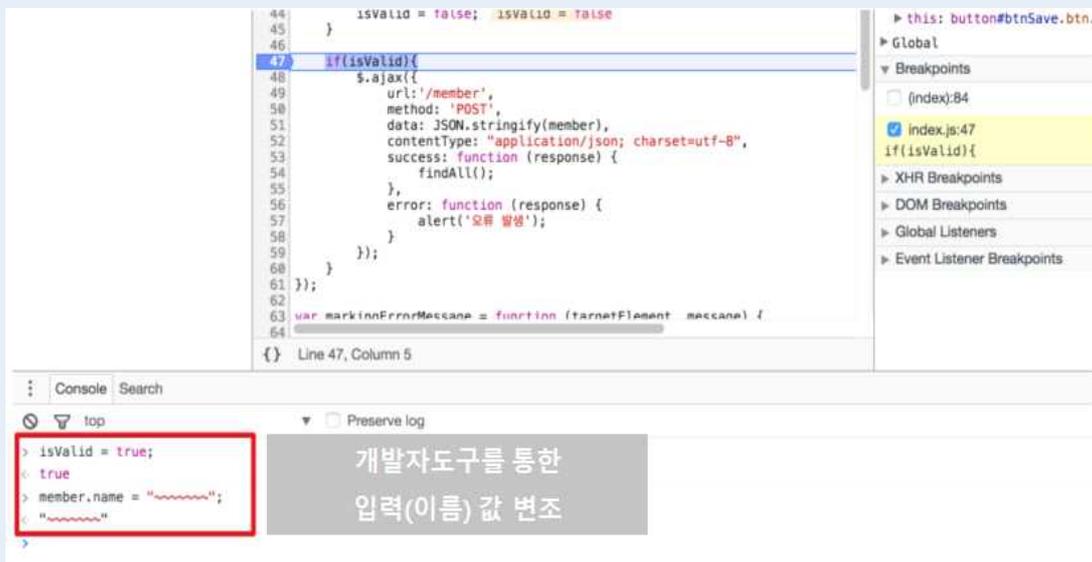
## 🔗 도입 시 유의사항

- 조희화면 보호의 경우 카메라, 스캐너를 통한 촬영, 복사하거나 일부 가상, 원격 데스크톱에서 보안성이 떨어지는 문제가 있어 보안 효과 보다 이용자의 서비스 사용시 불편 초래
- 서버를 통한 유효성 검증 개발 시 부하 증가에 따라 기본적인 유효성 검증은 클라이언트 우선 처리 권장
- 서버 유효성 검사의 경우 클라이언트 서버 아키텍처, 서버 개발 언어, 데이터 전송 방식에 따라 적절한 유효성 검사 방식 확인 필요
- 화면캡처 프로그램 제어, 브라우저 메뉴 제어, 프린터 제어 방지는 웹표준으로 구현 불가

### 💡 클라이언트·서버 유효성 검증

유효성(effectiveness) 검증이란 요구된 양식의 값이 화면상에 제대로 입력되고 서버에 전송되었는지 확인하는 것으로, 클라이언트 측에서는 주요 상수 및 변수, <input> 태그의 입력 값 및 패턴 속성 확인을 통한 유효성 검증 코드를 작성해야하며, 아래와 같은 이유로 서버측에서도 전송된 값에 대한 유효성 검증을 같이 수행해야함

- 매크로 등을 통한 중복 데이터 전송에 따른 서버 과부하 및 전송 지연
- 변조된 값을 위장하여 직접 서버로 전송하고 반환된 결과 값 수신
- 자바스크립트 오류로 인한 에러 값 전송에 따른 서버 오류 발생
- 개발자 도구(디버깅 도구)나 소스 보기에서 자바스크립트 입력 값 변조(회피)



| 그림 30 | 개발자 도구를 통한 입력 값 변조 예시

### ☀ 클라이언트 유효성 검증 방식

- 입력 값의 형식, 길이 등과 속성값등의 기본적인 유효성 검사
- 입력 조건 및 제약 조건(소프트웨어 로직)을 통한 유효성 검사
- 오류, 중복 입력된 데이터에 대한 예외처리
- 정규표현식을 통한 유효성 검사 처리

### ☀ 서버 유효성 검증 방식

- 동일한 IP에서 다량의 계정 접속이 이뤄지거나, 하나의 ID로 여러 접속이 발생하는 경우 등 어뷰징 패턴 방지(캡차와 같은 자동 생성 방지 기능 도입 고려)
- 서버에서 입력 조건과 제약 조건에 대해 유효성을 검증하는 코드 작성(클라이언트 유효성 검증 방식과 중복 개발)
- 서버 쪽에서 중복 입력, 유효성 검사(대부분 Form Validation이라고 함)를 수행하고 각 입력 값의 유효성 검사 결과 후 정상적인 데이터를 DB에 저장(위조, 예외, 오류의 경우 에러 처리)
- 클라이언트에서 입력, 전송되는 값의 유효성 검사 결과를 이용자 웹페이지를 통해 이용자에게 실시간으로 표시해주는 기능 개발(위조 시도에 대한 경고 통지)
- 이용자 이중 로그인(브라우저 별)이나 동영상 스트리밍 시간에 대한 유효성 검증 시 주기적으로 클라이언트가 서버에 폴링하여 사용 이력(로그) 정보를 얻어와 쿠키에 저장하고, 가장 최근 서버 정보의 유효값과 쿠키 정보를 비교하는 유효성 검증 방식 개발
- 유효성 검증 결과 예외, 오류 값의 경우, 이용자에게 통지하는 소프트웨어 로직 개발(사전 에러 코드 정의를 통한 상담원 QA 대응 지원)

## ■ 웹폼 문서 뷰어

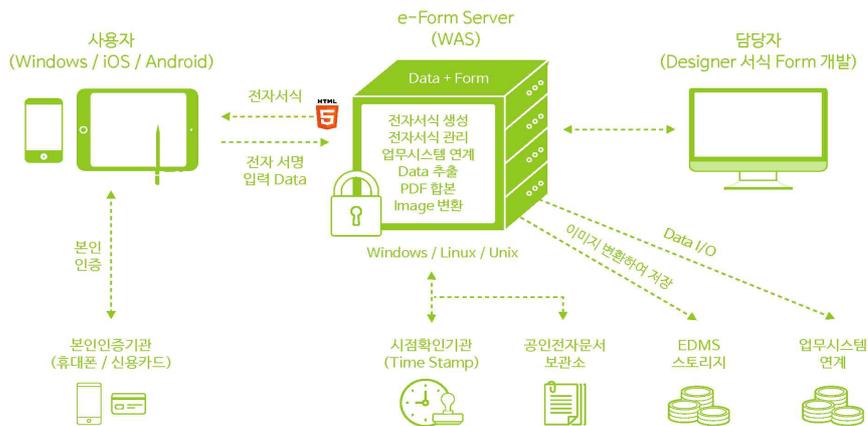
### 🔗 기술 개요

다양한 리소스(DB, CSV, XML, JSON, SAP 등)에서 추출된 데이터를 전자서식 서버를 통해 사전에 작성한 민원(신청서, 증명서 등)서식에 맞춰 웹폼 형태로 데이터와 서식을 조합해서 최종서식을 웹페이지 형태로 표출  
전자서식 서버는 대부분 웹서버와 HTML5 기능 활용을 통해 웹페이지 형태로 전자문서를 조회할 수 있는 기능 제공

위변조 방지 솔루션이나 전자서명 서버와 연계시 웹폼을 PDF로 변환 후 PDF 전자문서 형태로 연동 제공

### 🔗 적용 방법

웹폼은 대부분 상용 솔루션 형태로 제공하며, 솔루션은 전자서식(웹폼) 서버, 웹폼 디자이너(서식 에디터), 웹폼 뷰어로 구성되며, 전자서식 생성, 전자서식 관리, 업무 시스템 연계, 위변조 방지 솔루션 연계 등의 기능을 제공



| 그림 31 | 웹폼 서비스 프로세스

- 웹폼 서버 설치 매뉴얼에 따라 WAS 서버나 웹서버에 모듈 탑재
- 웹폼 서식 에디터를 통해 전자 서식 작성 및 웹폼 서버 서식 저장
- 위변조 방지(2D바코드, 시점인증, 워터마크) 솔루션 연동 시 PDF 변환 후 연동 추가 개발(PDF 문서와 동적 XML 서식 동시 변환을 통해 PDF, TIFF, HWP, XLS, DOC 파일 형식 저장 기능 지원)

- 웹폼 필요에 따라 그래프, 차트 등의 함수 조건 값이나 계산식 적용
- 서버 성능 저하시 로드밸런싱을 통한 성능 최적화 필요
- 운영기관 서비스 필요에 따라 본인인증기관, 시점확인기관, 전자서명서버, 공인전자문서 보관소, 업무시스템 등과 연계 개발 필요

■ 계약자 인적사항

성명	주민등록번호
홍길동	730402-1*****

■ 보장성보험(장애안전용보장성보험) 납입내역 (단위 : 원)

종류	상호	보험종류	주최보험자	납입금액	
	사업자번호	증권번호	증권보험자		
보장성	한국화재상해보험(주)	다이렉트개인용 자동차보험	730402-1*****	홍길동	177,910
	114-86-04***	A08110806***			
보장성	메리츠화재해상보험(주)회사	알파Plus보장0808	730402-1*****	홍길동	232,200
	116-81-03***	6A572***			
보장성	현대화재(주)다이렉트자동차보험(주)회사	개인용(Basic)	730402-1*****	홍길동	538,030
	201-81-95***	C20090579***			
보장성	이베리카인타세날이슈어런스(주)회사	(무) AIG 든든2	730402-1*****	홍길동	119,790

| 그림 32 | 웹폼 문서뷰어 적용 화면 예시

간단한 웹 문서 서식 출력의 경우 상용 솔루션 대신 CSS Print Stylesheet를 이용한 인쇄 레이아웃 설정 방식이나 서버에서 만든 웹페이지나 이미지(PNG, JPG)를 Canvas에 표시하고 출력하는 방식으로 구현 가능

### 🔗 도입 시 유의사항

- 서버에서 웹폼, PDF 서식 생성 및 문서 변환이 이루어지므로 기존 플러그인사용 방식보다 서버 부하가 증가하여 응답시간 지연 가능성 존재
- 부하 증가가 예상되는 경우, 문서 열람 서비스 처리 요청 즉시 조회가 아닌 조회리스트 제공 후 사용자 선택에 따른 문서조회 적용 권장(변환작업이 완료되면 리스트 표출)

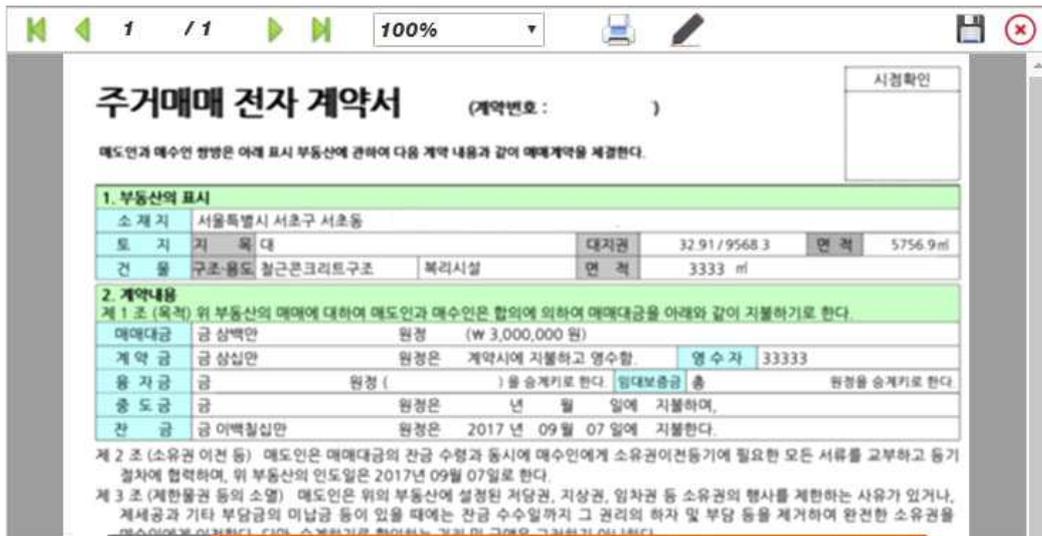


| 그림 33 | 증명서 조회 순차 적용 화면(출처 : 홈택스)

- 웹폼 솔루션을 활용하지 않고 직접 이미지나 웹페이지를 웹브라우저(Internet Explorer)에서 프린터로 출력할 경우 문서 상/하단에 사이트의 URL이 표시됨

## 🔗 적용 사례

- 국토교통부 부동산전자계약



| 그림 34 | 부동산 임대차 전자계약서 웹폼 화면 예시

## ■ 서버 기반 PDF변환 및 브라우저 내장 PDF 뷰어

### 🔗 기술 개요

다양한 리소스(DB, CSV, XML, JSON, SAP, HWP 등)의 PDF 문서 변환은 서버 변환 방식과 브라우저에서 XML문서를 바로 PDF로 렌더링하는 방식이 존재

브라우저 PDF 렌더링의 경우 오픈소스 자바스크립트 라이브러리(PDF.js)나 다양한 문서 포맷 변환을 지원하는 ViewerJS (<http://viewerjs.org/>) 활용

브라우저에서 PDF파일을 보여주기 위한 방법으로 과거엔 Adobe PDF Reader와 같은 별도의 플러그인을 설치해서 보여주었지만 현재 크롬, 엣지, 파이어폭스, 사파리 브라우저는 PDF 뷰어 기본 내장(다만 IE9, 10, 11 브라우저의 경우 Adobe PDF Reader를 사전 설치 후 브라우저 연동 사용)

PDF 뷰어의 조희화면 보호 기능(마우스제어, 특정 키보드 제어, 캡처방지, 개발자 도구 열람 방지 등)이 필요할 경우 PDF 표준 DRM 적용 가능

### 🔗 적용 방법

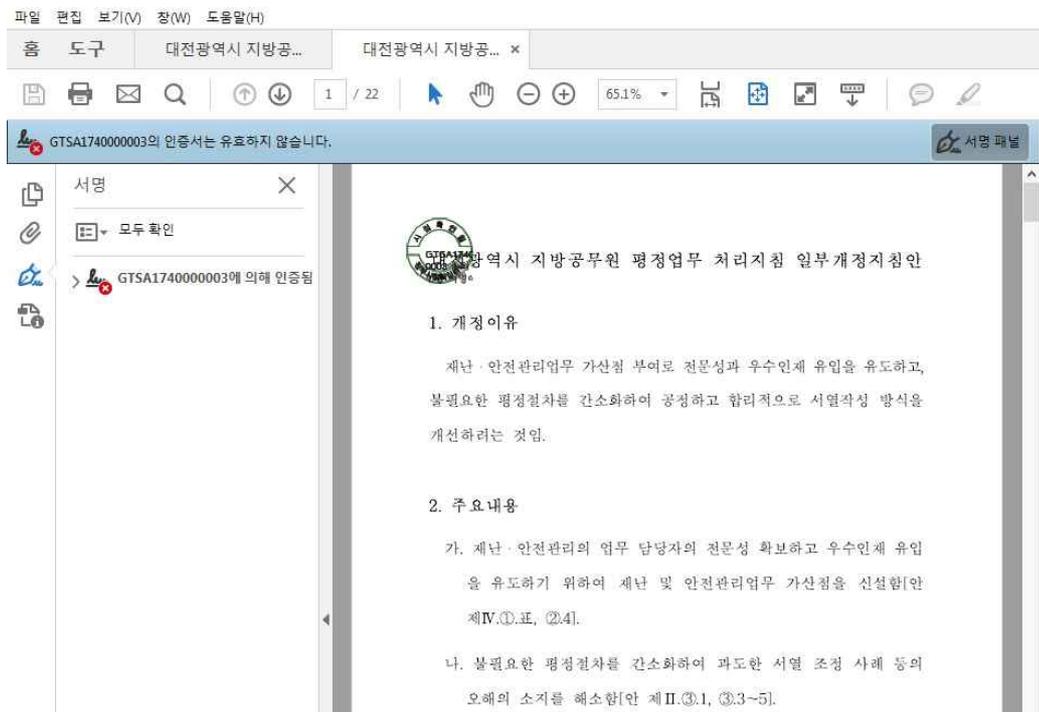
- 서버기반의 PDF 변환 솔루션을 통해 HWP, MS 오피스, XML 등 다양한 문서 형태를 PDF로 변환 가능(PDF.js와 같은 브라우저 렌더링 라이브러리를 통해 브라우저 내에서 변환이 가능하나, 복잡한 서식의 경우 변환 성능 문제 발생)
- PDF 기술 표준 규격 지원 확인(ISO 19005-1 호환 PDF / A-1a 및 -1b, ISO 19005-2 호환 PDF / A-2u 및 -2b, ISO 19005-3 호환 PDF / A-3u 및 -3b 중 브라우저 사양 별 지원 규격 확인)
- 크롬, 엣지, 파이어폭스, 사파리, 웨일 브라우저는 브라우저 내장 PDF를 활용하여 iframe 태그, src 속성에 PDF 파일 경로를 표시하면 브라우저 내에서 PDF 파일 호출 후 뷰어 가능
- IE 9, 10, 11 브라우저의 경우 데이터 형태의 PDF를 object tag의 data 속성을 이용, PDF 파일로 만들어서 URL Scheme을 통해 외부 Adobe PDF Reader를 호출하여 PDF 파일에 문서 뷰어
- 대부분 문서 변환 안전성 및 지속적인 유지보수 이유로 상용 솔루션을 적용하고 있으나, ng2-pdf-viewer와 같은 오픈소스를 통한 PDF 변환도 가능

## ☞ 도입 시 유의사항

- 서버에서 웹폼, PDF 서식 생성 및 문서 변환이 이루어지므로 기존 플러그인사용 방식보다 서버 부하가 증가하여 응답시간 지연 가능성 존재
- 부하 증가가 예상되는 경우, 문서 열람 서비스 처리 요청 즉시 조회가 아닌 조회 리스트 제공 후 사용자 선택에 따른 문서조회 적용 권장 ( 변환작업이 완료되면 리스트 표출)
- PDF 변환 시 개인정보 필터링(개인정보 제거) 권장
- 오픈소스를 활용한 전용 PDF 뷰어를 개발할 경우 라이선스 정책 및 유지보수 방안 마련 필요
- 브라우저 내장 PDF를 활용하여 PDF문서를 열람하는 경우, PC에 PDF문서가 임시 저장되므로, PDF 생성시 열람용 암호를 설정하고, 문서열람 시 암호 입력 후 열람·출력하는 기능 검토·적용 권장

## ☞ 적용 사례

- 정보공개포털 원문정보 상세조회, 홈택스 연말정산 등



| 그림 35 | 서버 기반 PDF 변환 및 내장 PDF 연동 예시(출처 : 정보공개포털)

## ■ 서버 기반 시점 확인

### 🔗 기술 개요

기존 시점확인을 위한 TSA Client 플러그인의 5가지 기능을 서버에서 지원할 수 있도록 개발(현재 대다수의 시점 확인 솔루션은 서버 방식으로 개발)

- 사용자 인증 : 이용자가 본인의 신원확인 기능(인증서버 연동 지원)
- 무결성 : 원문 내용의 진본 여부 및 위변조 여부 확인 기능
- 적시성 : 전자서명 시점에 행위가 발생했음을 확인하는 기능
- 부인방지 : 전자서명 행위에 대한 부인을 하지 못하게 방지하는 기능
- 장기검증 : TSA의 유효기간 한정 및 만료 후에 서명 검증 기능

시점 확인은 전자문서(PDF)의 진본확인 기술규격을 이용하여 전자문서(PDF) 내에 진본확인 마크 인영 등 시점확인(Time Stamp) 토큰 검증 및 확인에 필요한 부가정보를 주입(시점 확인 기술 규격은 PDF 표준 규격으로 지원)

### 🔗 적용방법



▣ 그림 36 | 전자문서진본확인시스템(GTSA) 서버 연동 지원(출처 : 행정안전부)

- 공인 시점확인 서비스를 도입할 경우 전자문서(PDF품 생성) 서버와 행정전자서명 인증관리센터(공인인증기관)의 행정 전자서명 인증표준보안 API를 통해 전자문서진본확인센터 시스템과 연동(서버연계 방식)

- 전자문서 서버에서 전자문서진본확인센터 연동 후 타임스탬프 이미지 발급(생성) 및 PDF 파일에 이미지 삽입 기능을 서버에서 수행(전자문서 위변조 방지 솔루션 중 서버 변환 방식 지원 여부 확인 필요)
- 타임스탬프 검증 기능(검증자)은 전자문서진본확인센터의 검증용 소프트웨어 설치 후 PDF 문서 내 타임스탬프의 위변조 여부를 검증하거나 서버에서 타임스탬프가 적용된 PDF를 업로드, 검증 후 검증 결과를 통보하는 방식으로 개발이 가능함

### 🔗 도입 시 유의사항

- 타임스탬프 기능은 전자문서 서버 및 리포팅툴 서버나 위변조 방지 서버 솔루션에서 기본 기능으로 지원하는 경우가 있어, 솔루션 도입 시 확인 필요
- GTSA 규격을 지원하는 PDF Reader나 브라우저 내장 PDF 규격 확인 필요
- 시점확인 기능은 ISO 32000-1 전자서명 표준을 지원하는 PDF 리더 사용 필요
- PDF 표준을 지원하는 뷰어에서 시점확인 기능 지원 시 시점확인 S/W를 추가 설치하는 방식으로 제공 가능

### 🔗 적용 사례

- 국세청 연말정산 간소화 시점확인, 정보공개포털 원문정보 조회, 환경민원포털 온라인 환경민원 발급, 신한생명 전자청약 등



| 그림 37 | 연말정산 간소화 PDF 파일 시점 확인 적용 예시

## 7 출력물 위변조 방지 및 프린터 제어

### 개요

인터넷을 통한 본인확인 후 발급되는 증명서 등 출력물에 대한 위·변조 방지(2D 바코드, 워터마크, 복사방지마크, 전자관인, 프린터 스푼접근제어 등)와 발급매수당 수수료 징수를 위한 프린터 제어 기능을 활용하기 위해 플러그인 사용

### 플러그인 사용 현황

#### 출력물 위변조 방지

- 전자문서 위변조 방지 플러그인의 경우 2차원 바코드, 워터마크, 복사방지마크, 시점확인을 통한 출력물 진본성 보장 및 출력물 내용 검증을 지원하는 프로그램
- 이외 문서확인(발급)번호, 음성바코드 정보 등을 출력물에 표시하는 기능 지원

**인터넷문서확인번호(문서발급번호)**  
증명서의 진위 여부를 확인 할 때 사용하는 고유문서확인(발급)번호.

**안내 문구**  
인터넷으로 발급된 증명서임을 나타내는 메시지와 수령 기관의 원본 대조가 가능하도록 안내 문구 삽입.

**복사방지마크**  
원본 증명서에 삽입된 코드의 변화를 육안으로 확인하여 문서의 원본여부 확인

**행정 효율과 협업 촉진에 관한 규정 제36조(등록)**  
③ 행정기관의 장은 관인을 위조·변조하거나 부정하게 사용하지 못하도록 필요한 조치를 하여야 한다.

**전자관인**  
워터마크를 이용하여 중요 정보 은닉 전자서명이 암호화되어 있음

**2차원 바코드**  
원본 증명서의 내용과 발급 기관 전자서명을 수록하고 있으며, 스캐너를 통해 발급 증명서의 원본을 복원 해내는 방법으로 위·변조 여부 확인

| 그림 38 | 4대보험 완납 증명서 출력문서 위변조 방지 예시

#### 프린터 출력 제어

범용 프린터 드라이버 제어, 스푼(Spool) 파일 유출 방지, 공유/가상 프린터 제어, 발급 매수 제어를 위한 프로그램

〈표 11〉 위변조 방지 및 프린터 출력제어 상세 설명

기능	상세 설명
2D 바코드	문서의 내용을 2차원 바코드로 표현하여 출력물 진본성 보장
복사방지마크	원본 증명서에 삽입된 코드의 변화를 육안으로 확인하여 문서의 원본여부 확인
워터마크	기관의 로고/직인 등의 이미지에 워터마크를 이용하여 중요 정보 은닉, 2차원 바코드 훼손 시 워터마크를 이용하여 체크
화면캡처방지	웹브라우저(뷰어)에서의 인쇄, 저장, 복사 방지 마우스 오른쪽 버튼의 팝업메뉴 통제
프린터제어	범용 프린터 드라이버 제어 및 스푼(Spool) 파일 유출 방지 공유/가상 프린터를 이용한 출력 제어 및 발급 매수 제어
프린터 발급매수 제어	유료 발급의 신청한 매수만 출력할 수 있도록 출력매수 제어

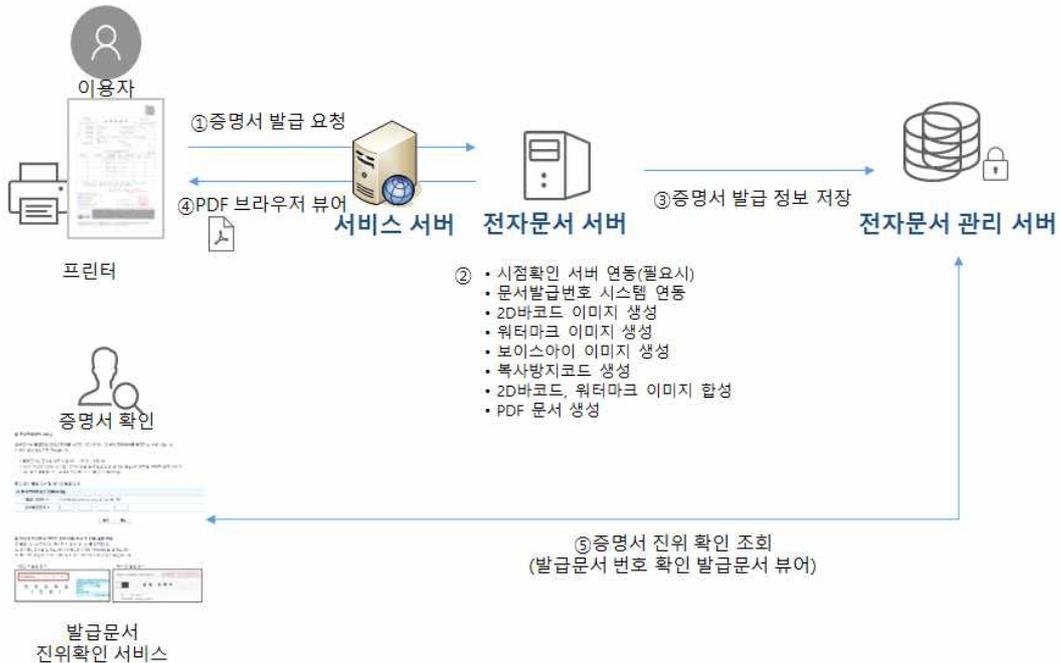
**대체 기술**

**서버 기반 출력물 위변조 방지**

**기술 개요**

기존 이용자 PC의 플러그인에서 수행하던 출력물 위변조 방지 기능을 서버에서 수행할 수 있도록 전환

운영기관의 (웹)서비스 서버에서 전자문서 서버와 연계를 통해 PDF 파일 수신 후 전자문서 위변조 방지를 위한 이미지 생성 및 합성



| 그림 39 | 플러그인 무설치 전자문서 위변조 시스템

## 🔗 적용 방법

기존 PC 플러그인 형태의 위변조 방지 솔루션을 서버 방식으로 전환개발하거나 신규 서버 솔루션 도입

PC에서 수행했던 PDF변환, 2D 바코드 이미지 생성 삽입, 문서 위변조 방지 기능을 서버에서 수행

PDF 문서 변환 시 서버에서 위변조 이미지를 생성, PDF 파일로 병합 후 출력하는 방식으로 아래와 같이 개선하고 시점확인 등도 서버에서 수행하도록 전환

- 전자문서 위변조 방지 시스템을 구성하는 문서 신청 시스템, 문서 발급 시스템, 문서 관리 시스템에서 기존 이용자 PC에 설치했던 위변조 방지 플러그인 기능을 이전해서 추가 개발
- 문서 신청 시스템에서 웹폼 서버나 PDF 변환 서버와 연동을 통해 위변조 방지 기능이 적용되지 않은 문서 수신
- 문서 발급 시스템에서 수신한 PDF 문서 서식 및 내용 Parsing 후 2차원 바코드 및 복사방지마크(기관장 관인 포함) 이미지 생성
- PKI 기반 전자서명/시점확인 시스템 연동
- 발급문서 번호 생성, 합성 시스템 연동
- 문서 관리 시스템에 발급된 PDF 문서 서식 및 메타 정보 저장
- 문서 관리 시스템을 통해 위변조 방지 솔루션이 적용된 PDF 생성 후 이용자 브라우저의 내장 PDF 뷰어에 출력

## 🔗 도입 시 유의사항

- 서버에서 위변조 이미지 생성 및 합성이 이루어지므로 기존 플러그인사용 방식 보다 서버 부하가 증가하여 응답시간 지연 가능성 존재
- 부하 증가가 예상되는 경우, 문서 열람 서비스 처리 요청 즉시 조회가 아닌 조회 리스트 제공 후 사용자 선택에 따른 문서조회 적용 권장 ( 변환작업이 완료되면 리스트 표출)

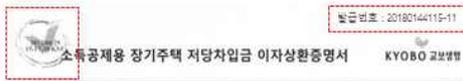
- 진본확인을 위한 2D바코드는 진위확인을 위해 스캔을 통한 전자화파일로의 변환작업과 별도의 검증프로그램이 필요하여, 번거로움으로 인해 실제 활용되는 경우가 극히 적음(진위확인번호를 통한 진본확인방식이 보다 간편하여 활용성 높음)
- 출력 문서 이외에 위변조 방지 기능이 불필요 할 경우 플러그인 제거, 인터넷 열람(화면조회)시에는 위변조 방지 불필요
- 음성 바코드의 경우 장애인 선택 이용자의 경우에만 2D 바코드 적용 검토(서버 용량 경감 조치)
- 복사방지마크는 프린터 최적화된 값으로 출력이 불가하여 복사 방지 기능에 대한 효과가 적다고 알려져 있음

## 적용 사례

- 교보생명 증명서 발급, 우리은행 입출금 내용 증명

### 시점확인

전자문서 생성시점의 법률적 증명과 위·변조 방지를 위해 특정 시점에 존재하였으며, 이후 변경되지 않음을 증명



발급번호 : 20180744115-11

### 문서발급번호

증명서의 진위 여부를 확인 할 때 사용하는 고유문서확인(발급)번호.

연차별입금			
연월	주입금액(천원)	잔액(천원)	잔액(천원)
2012-03			
2012-04			
2012-05			
2012-06			
2012-07			
2012-08			
연간합계액			
소액공제대상액			

년도 소액공제용 장기주택 저당차입금 이자 상환현황			
상환월	위 차	상환월	위 차
2012-03			
2012-04			
2012-05			
2012-06			
2012-07			
2012-08			
연간합계액			
소액공제대상액			

\* 이자상환증서란 이차금융권 발행된 주택차입금(주택담보대출)의 이자상환액(이자, 발행일, 채무자, 주기로 납입할) 중 주택공제용 장기주택 저당차입금에 해당되는 이자상환액에 대해 발급된 증명서입니다. 소액공제대상액에 대해 위 차(연월) 및 소액공제대상액에 대한 위 차(연월)에 대한 증명서를 발급합니다. 장기주택저당차입금에 대한 위 차를 위 차의 금액 상환하였음을 증명하여 주시기 바랍니다.

신청인

위와 같이 장기주택저당차입금에 대한 이자를 상환하였음을

\* 실제 발급 보행료의 소액공제대상 보행료는 다를 수 있습니다.

\* 상기 내용은 교보생명 홈페이지(www.kyobo.co.kr)에서 확인 가능합니다.



### 2차원 바코드

원본 증명서의 내용과 발급 기관 전자서명을 수록하고 있으며, 스캐너를 통해 발급 증명서의 원본을 복원 해내는 방법으로 위 변조 여부 확인

교보생명보험주식회사

홈페이지: www.kyobo.co.kr / 고객센터: 1599-0000

| 그림 40 | 서버기반 위변조 방지(출처 : 교보생명)

## ■ 발급문서 진위확인 서비스

### 🔗 기술 개요

온라인으로 발급한 민원증명서를 수령한 기관/개인이 발급문서의 진위여부를 확인하는 서비스로 대부분의 발급문서는 접수 후 일정기간 동안 진위확인 지원

민원증명서 생성시 진위확인번호를 기재하고, 운영기관 서버에 발급된 민원증명서 사본을 저장함

기관/개인이 수령한 민원증명서에 기재된 진위확인번호로 서버의 민원증명서를 열람하고, 수령한 민원증명서와 내용을 비교하여 위변조 여부를 확인할 수 있음

### 🔗 적용 방법

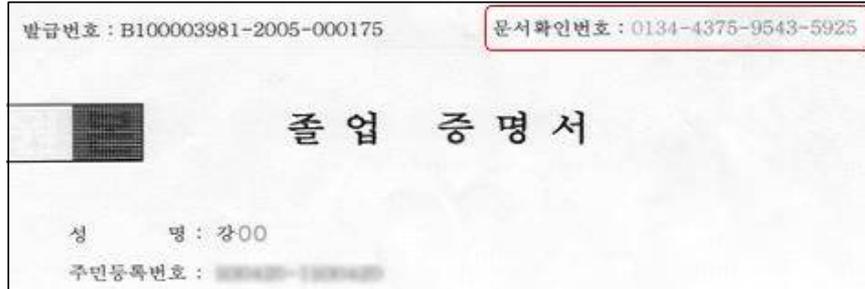
#### ○ 진위확인번호 발급·기재

- 레포팅툴(전자문서) 서버를 통해 문서확인번호 생성 및 문서 합성
- 레포팅툴 서버가 없을 경우, 별도 진위확인 서비스 서버 개발을 통해 문서확인번호 생성 및 적용(최소 12자리 이상, 숫자나 숫자+영문자 결합)하거나 발급 일자 와 발급/문서확인번호를 함께 입력하도록 개발)
- 문서확인번호 단일 기재 방식 : 인터넷발급(프린터출력) 요청시 난수와 시점 정보를 결합하여 문서확인번호 생성 후 전자문서 출력 시 입력



| 그림 41 | 문서확인번호 단일 기재 방식

- 발급 번호+문서확인번호 이중 기재 방식 : 인터넷발급(프린터출력) 요청시 순차적인 시점 정보 기반 문서발급번호와 난수 기반의 문서확인번호를 동시에 생성한 후 전자문서 출력 시 입력



| 그림 42 | 발급번호+문서확인번호 이중 기재 방식

- 인터넷 발급(프린터출력) 요청시 발급일자와 문서확인번호를 동시에 생성 후 발급일자와 문서발급번호로 확인 서비스 제공 방식

| 그림 43 | 발급일자+증명서 발급번호 방식

- 공통적으로 문서 진위 여부를 검증 확인할 수 있는 문서확인번호 조회 서비스 페이지 개발 필요

## ☞ 도입 시 유의사항

- 진위확인 번호 발급 서비스와 검증 서비스 동시 제공 필요
- 스토리지 용량 검토 후 발급문서 진위확인 유효기간 자체 산정
- 발급문서 확인번호에 붓이 접근해서 난수로 확인 번호를 조회하는 걸 방지하기 위해 보안문자 입력(캡차) 등의 보완 조치 가능

| 그림 44 | 캡차 적용 발급 문서 진위 확인서비스

## 🔗 적용 사례

- 민원24 문서진위확인 서비스, 홈택스 문서진위확인 서비스 등 증명서 발급 사이트

**1 문서진위확인 서비스**

온라인으로 발급받은 민원증명서를 수령한 기관/개인이 문서의 진위여부를 확인하는 서비스입니다.  
아래와 같은 방법으로 가능합니다.

- \* 발급문서는 접수일 이후 90일까지 조회가 가능합니다.
- \* KLS, 지방인사정보 시스템, 식약처 등을 통해 발급 받은 문서는 발급사이트를 기타로 선택 하세요.
- \* 국세청 민원증명서는 [국세청 발급문서] [이동]을 선택하세요.

**2 민원24 발급 문서 및 타기관 발급 문서**

※ 문서확인번호를 입력하세요.

발급 사이트 *	<input type="radio"/> 민원24(www.minwon.go.kr) <input checked="" type="radio"/> 기타
문서확인번호 *	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>

**3 인터넷 발급문서 확인을 위한 입력 순서 및 입력 요령 안내**

- ① 발급 사이트(민원24, 국세청 제외 타사이트)를 선택합니다.
- ② 문서확인번호를 입력합니다. (국세청은 아래의 이동버튼을 클릭합니다.)
- ③ 문서확인번호의 위치는 아래의 예시 이미지의 위치 안내를 참고합니다.

>민원24 발급 문서



>타기관 발급 문서



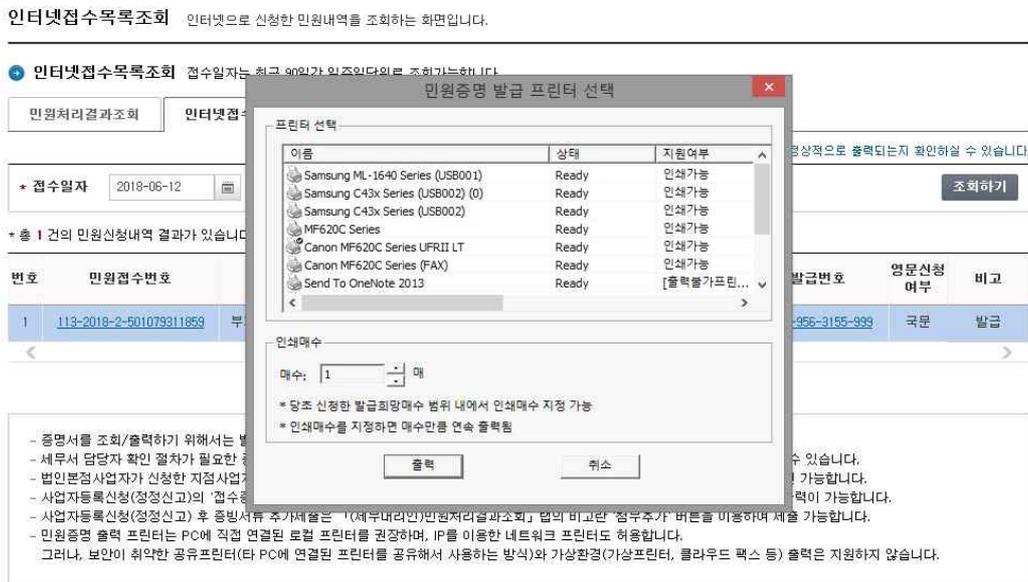
| 그림 45 | 민원24 온라인 발급 문서진위확인 서비스 예시

## ■ 브라우저 내장 프린트 기능

### 🔗 기술 개요

웹폼, PDF 전자문서 출력 시 브라우저 내장 프린트 기능을 호출하여 출력하는 방식

기존 범용 프린터 드라이버 제어 및 스푼(Spool) 파일 유출 방지, 공유/가상 프린터를 이용한 출력 제어 및 발급 매수 제어를 위해 사용 했던 플러그인을 설치하지 않고 브라우저가 지원하는 기본 프린터 기능을 사용하여 출력



| 그림 46 | 출력 가능 프린터 리스트 제어 플러그인

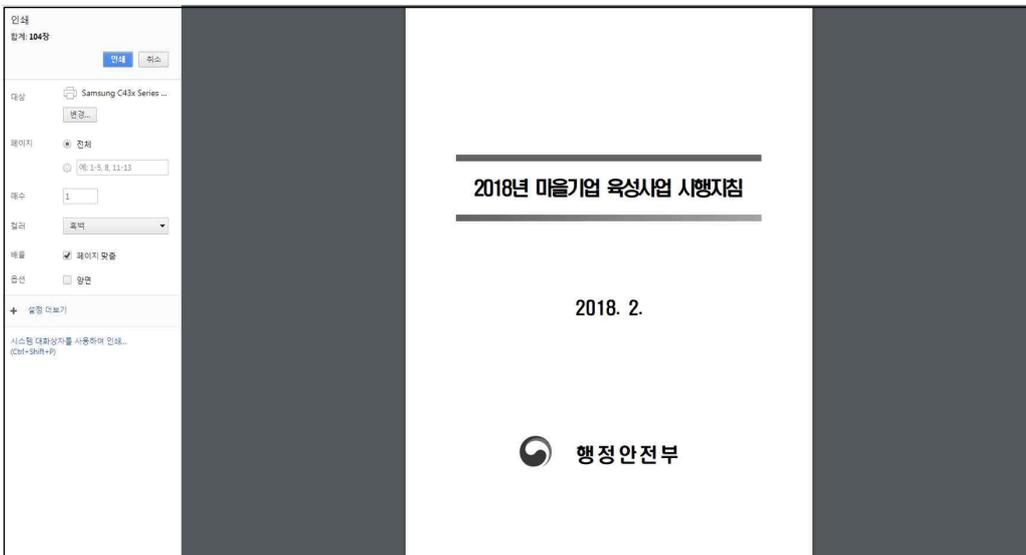
### 🔗 적용 방법

- 웹폼(웹페이지), PDF 파일을 브라우저에서 조회하고 기본 프린터 출력 메뉴 및 브라우저가 지원하는 출력 가능 프린터 리스트로 출력  
단, 유료 증명서 발급을 위한 발급 매수 제한이 필요한 경우 플러그인을 설치하여 매수 제한 발급 구현
- 기존 기관이 허용한 프린터만 출력 가능한 방식의 프린터 제어 정책을 브라우저가 지원하는 출력 가능 프린터 리스트로 출력하는 방식으로 출력에 대한 제한을 없애고, 출력 매수에 따른 과금을 위한 제어도 증명서 무료화 유도를 통해 플러그인 없이 프린터 출력 지원 검토

## 🔗 도입 시 유의사항

- IE 브라우저에서 웹폼이나 웹페이지 출력 시, 상·하단에 URL 정보가 출력됨에도 문서 유효성 인정 여부 검토 필요
- 현재(2018년 9월) “민원 처리에 관한 법률 시행령” 제30조 출력 매수의 제한조치가 의무화되어 있으므로, 출력매수 제한 플러그인을 제거할 수 없음
- 출력 매수의 제한조치 의무화를 삭제하도록 법령 개정이 추진 중이므로, 향후 신규 공공 웹사이트 구축을 하거나 기존 공공 웹사이트의 플러그인을 제거할 경우, 관련 법령 개정 여부를 확인하고 제거시점의 규정에 적합한 플러그인 대체(제거) 방안을 선택하는 것을 권장

## 🔗 적용 사례



| 그림 47 | 크롬 브라우저 내장 PDF 뷰어를 통한 전자문서 출력

### 개요

비디오/오디오와 같은 멀티미디어 기능과 파일처리, 리포팅툴, 웹에디터 등은 HTML5 표준 규격 제정 이전에는 플러그인을 보편적으로 사용

HTML5 표준이 브라우저에 적용된 2015년 이후 아래와 같은 기능은 웹표준으로 구현 가능

- 멀티미디어를 위한 비디오/오디오 재생
- PC 카메라/마이크 제어
- 멀티파일 업로드/다운로드(Drag&Drop)
- 애니메이션, 그래픽, 차트, 벡터그래픽(Canvas, SVG, CSS3, WebGL)
- 통계 그리드, 그래프, 문서 레이아웃, 웹에디터 등 리포트 템플릿 작성

### 플러그인 사용 현황

#### ■ 멀티미디어(Flash Player, Silverlight, Java Applet, 퀵타임, 윈도우 미디어 플레이어)

- Rich Internet Application이라고도 하며, 비디오 및 오디오 스트리밍, 애니메이션, 벡터 그래픽 등에 사용하기 위한 프로그램

#### ■ 플러그인 방식 리포팅툴, 웹에디터

- 업무에 필요한 다양한 리포트 서식 저작 기능을 제공, 웹 개발 생산성을 높이고, 다양한 UI/UX 화면을 손쉽게 개발하도록 지원

#### ■ 플러그인 방식 그래픽 및 그리드(Flash Player, Silverlight)

- 웹사이트에 차트, 그리드, 애니메이션, 벡터 그래픽, 동적인 반응형 사용자 이벤트 지원을 위해 사용하는 프로그램

#### ■ 플러그인 방식 파일처리

- 이용자의 증명서 및 기타 파일들에 대해 멀티 파일 업로드, 폴더 업로드, 대용량(고속) 파일 업로드, 특정 확장자 업로드, 고속 파일 다운로드 기능 지원을 위해 파일 업로드/다운로드 플러그인 사용

## 대체 기술(웹표준)

### 멀티미디어

플러그인 설치없이 HTML5 표준 기술로 다음 멀티미디어 요소 및 API를 이용하여 개발하거나, 오픈소스 멀티미디어 라이브러리, 외부 동영상 서비스 링크를 이용하여 대체할 수 있음.

#### HTML5 기술을 활용한 개발

- 동영상, 음성 재생

<video> 요소, <audio> 요소

```
<video>
  <source src="movie.mp4" type="video/mp4"></source>
  <source src="movie.ogv" type="video/ogg"></source>
  <source src="movie.mpeg" type="video/mpeg"></source>
</video>
```

```
<audio controls="controls">
  <source src="Kalimba.mp3" type="audio/mp3" />
  <source src="Kalimba.ogg" type="audio/ogg" />
</audio>
```

단순 플레이는 지원하나 고급 기능들은 브라우저 별 지원 여부 확인 후 개발 필요

Feature	Chrome	Firefox (Gecko)	Internet Explorer	Opera	Safari
Basic support	3.0	3.5 (1.9.1)	9.0	10.50	3.1
<audio>: PCM in WAV	(Yes)	3.5 (1.9.1)	No support	10.50	3.1
<audio>: Vorbis in WebM	(Yes)	4.0 (2.0)	No support	10.60	3.1[1]
<audio>: Streaming Vorbis/Opus in WebM via MSE	?	36.0 (36.0)[2]	?	?	?
<audio>: Vorbis in Ogg	(Yes)	3.5 (1.9.1)	No support	10.50	No support
<audio>: MP3	(Yes)[4]	(Yes)[5]	9.0	(Yes)	3.1
<audio>: MP3 in MP4	?	?	?	?	(Yes)
<audio>: AAC in MP4	(Yes)[6]	(Yes)[7]	9.0	(Yes)	3.1
<audio>: Opus in Ogg	27.0	15.0 (15.0)	?	?	?
<audio>: FLAC	56.0	51 (51)	No support	No support	11
<audio>: FLAC in Ogg	56.0	51 (51)	No support	No support	No support
<video>: VP8 and Vorbis in WebM	6.0	4.0 (2.0)	9.0[8]	10.60	3.1[9]
<video>: VP9 and Opus in WebM	29.0	28.0 (28.0)[36]	?	(Yes)	?
<video>: Streaming WebM via MSE	?	42.0 (42.0)[35]	?	?	?
<video>: Theora and Vorbis in Ogg	(Yes)	3.5 (1.9.1)	No support	10.50	No support
<video>: H.264 and MP3 in MP4	(Yes)[3]	(Yes)[10]	9.0	(Yes)	(Yes)
<video>: H.264 and AAC in MP4	(Yes)[4]	(Yes)[11]	9.0	(Yes)	3.1
<video>: FLAC in MP4	62.0	51 (51)	?	?	?
any other format	No support	No support	No support	No support	3.1[12]

| 그림 48 | HTML5 멀티미디어 기능 요소 별 브라우저 지원 내역

☞ 브라우저 별 미디어 포맷 비교

[https://developer.mozilla.org/en-US/docs/Web/HTML/Supported\\_media\\_formats](https://developer.mozilla.org/en-US/docs/Web/HTML/Supported_media_formats)

기존 웹서버 설정을 통해 동영상 서버 구축이 가능하며, 트래픽이 많을 경우 스트리밍 서버 솔루션 도입을 통해 신규 구축 필요

- 실시간 동영상 통화/녹화 기술
  - WebRTC(Web Real Time Communication)
  - Media Streaming API
  - Media Capture API
- 이퀄라이저 등 음향 효과 기술
  - 웹오디오(Web Audio)
- 안정적 스트리밍 관리
  - MSE(Media Source Extensions)
- 콘텐츠 보호
  - EME(Encrypted Media Extensions)

#### ☀ 개발 참고 자료

한국인터넷진흥원 “인터넷 이용환경 개선을 위한 기술안내서(2016) 중 멀티미디어” 내용 참조

#### 🔗 오픈소스 멀티미디어 라이브러리 활용(유료 솔루션 포함)

HTML5 오픈소스 멀티미디어 플레이어 라이브러리 설치를 통한 서비스 제공(라이선스 및 유지보수, 유료 솔루션일 경우 도입 비용 확인)



| 그림 49 | video.js의 비디오 재생기

#### ☀ 오픈소스 멀티미디어 라이브러리 비교

<http://videosws.praegnanz.de/>

### 외부 동영상 서비스에 업로드 후 사이트에 링크 URL 적용

오픈소스(유료 솔루션) 도입이나 웹서버, 스트리밍 서버 구축이 어려울 경우나 코덱 변경이 어려울 경우 외부 동영상 서비스에 멀티미디어 콘텐츠 업로드 후 운영기관 웹페이지에 URL 링크를 통해 동영상 서비스 제공

## 리포팅툴 및 웹에디터

### 웹표준 솔루션 도입/전환

리포팅툴 및 웹에디터는 HTML5 웹표준 방식으로 개발된 리포팅툴 솔루션 및 웹에디터 솔루션 도입, 활용

## 그래픽 및 그리드(차트)

플러그인 형태로 그래픽, 그리드(차트)를 개발한 경우 HTML5 기반 웹표준 규격을 지원하는 웹사이트로 전환 개발, HTML5 벡터 그래픽, 그래픽 차트를 처리할 수 있는 SVG(Scalable Vector Graphics), 동적인 2D/3D 그래픽 Drawing 기능을 제공하는 Canvas, 애니메이션을 지원하기 위한 CSS3 Animation/ Transition 기술을 통해 전환

〈표 12〉 Canvas와 SVG 기능 비교

항목	<canvas>	<svg>
출력 방식	비트맵 이미지	벡터
비트맵 이미지 편집	가능	불가
성능에 미치는 영향	자바스크립트의 복잡도	하위 요소에 의존 (개수 등)
적용 대상	게임, 이미지 편집 등	그래프, 다이어그램 등

〈표 13〉 Canvas 및 SVG 라이브러리

라이브러리	주소	설명
rMate (상용)	<a href="http://www.riamore.net">http://www.riamore.net</a>	Canvas 기반 차트 Data Grid, Map Chart 조달 등록(국산)
Nwagon (오픈소스)	<a href="http://nuli.navercorp.com/s-haring/nwagon">http://nuli.navercorp.com/s-haring/nwagon</a>	네이버에서 만든 오픈소스 차트 추가적인 plug-in 없이 VML을 이용하여 IE 하위 버전 지원
Kinetic.js (오픈소스)	<a href="http://kineticjs.com/">http://kineticjs.com/</a>	Canvas 기반 객체 모델 지원 애니메이션 및 컨트롤 지원 다양한 입출력 관련 기능 제공
Createjs (오픈소스)	<a href="https://createjs.com/">https://createjs.com/</a>	Flash에서 지원하는 벡터, 비트맵, 트윈, 사운드, 버튼, 모션 안내선, 애니메이션 마스크를 Javascript Canvas로 제작 지원
Fabric.js (오픈소스)	<a href="http://fabricjs.com/">http://fabricjs.com/</a>	Canvas 기반 객체 모델 지원 SVG 입출력 제공
Three.js (오픈소스)	<a href="http://threejs.org/">http://threejs.org/</a>	Canvas, WebGL 기반 자바스크립트 3D 엔진 가장 범용으로 사용되는 순수 자바스크립트 3D 엔진
Babylon.js (오픈소스)	<a href="http://www.babylonjs.com/">http://www.babylonjs.com/</a>	Canvas, WebGL 기반 자바스크립트 3D 엔진
D3.js (오픈소스)	<a href="http://d3js.org/">http://d3js.org/</a>	데이터 라이브러리 시각화 라이브러리 데이터 트리본 모델 많은 차트 라이브러리들의 기반 소스로 활용
processing.js (오픈소스)	<a href="http://processingjs.org/">http://processingjs.org/</a>	Canvas 기반 Processing 문법 지원
paper.js (오픈소스)	<a href="http://paperjs.org/">http://paperjs.org/</a>	Canvas 기반 DOM 모델 지원 마우스 및 키보드 인터랙션 지원 벡터 모델 지원
Snap.svg (오픈소스)	<a href="http://snapsvg.io/">http://snapsvg.io/</a>	SVG 라이브러리 폭넓은 기능 지원 IE 하위 버전 지원 안함

## ■ 파일 업/다운로드

### 🔗 웹표준 솔루션 도입/전환

멀티파일 업로드/다운로드 기능을 지원하는 웹표준 라이브러리나 솔루션으로 대체 가능

HTML5 웹표준 방식을 지원하는 멀티파일 업로드 라이브러리 및 솔루션 사용

### 🔗 웹표준(File API)으로 구현

단순 파일 업로드의 경우 HTML5 File API를 통해 PC에 있는 바이너리 데이터와 특정 파일을 이용자가 선택해서 파일 업로드 제공 가능

파일을 업로드 하기 위해 웹사이트의 특정 영역으로 파일을 드래그하거나 <input>요소로부터 전달받은 파일 디렉토리 및 파일에 접근한 후 XMLHttpRequest를 사용해서 바이너리 파일을 업로드

File API를 이용하면 서버로부터 전송하는 썸네일 이미지 스트림을 파일로 생성하거나, 오프라인에서 사용자가 참조한 파일을 저장, 전송할 수 있으며, 특정 파일확장자나 MIME 타입을 확인하여 서버 업로드 제한 가능(SSL 보안 전송도 가능)

#### 💡 개발 참조

KS X OT2000, “HTML5 웹애플리케이션 개발 지침 4.4.7 File API”

## 원격제어

## ■ 사용 목적

- 원격제어 Protocol을 통해 PC나 스마트폰, 브라우저의 원격 제어 및 제어속도, 세션관리, 통화를 위한 기술로 운영기관에서 원격 접근을 통해 웹서비스 실행 및 문제 해결을 위해 원격지원을 위해 사용

## ■ 대체 방안

- 이용자 선택 설치

## 장치관리

## ■ 사용 목적

- 시스템(OS) 정보확인, 드라이버 접근, 메모리 커널 접근(백신, 방화벽, 키보드보안), IP 정보확인(조달 부문의 부정 입찰 확인), 맥어드레스 정보확인 등의 시스템 정보에 접근하거나 장치 제어가 필요할 경우 반드시 플러그인 설치
- 시스템 접근 중 카메라(미디어), GPS, 오디오, 센서는 W3C Devices and Sensors Working Group, W3C Geolocation Working Group, Generic Sensor API Working Group의 기술 표준화를 통해 웹기술로 개발 가능

 윈도우 운영체제에서 시스템 드라이버나 메모리와 커널에 접근하는 실행파일은 안전성과 보안성 보장을 위해 EV(Extended Validation) 인증서로 코드서명 후 승인/설치 권장

## ■ 대체 방안

- 웹표준으로 지원하지 않는 장치관리의 경우 이용자 선택 설치
- 웹표준을 지원하는 장치관리는 웹표준 기술로 구현

## 인증서 모바일 복사

## ■ 사용 목적

- PC에 보관된 공인인증서를 스마트폰의 공인인증서 앱으로 복사·저장하는 기능(스마트폰에 인증서 가져오기)을 제공

## ■ 대체 방안

- 공인인증서는 이용자 선택 설치
- 브라우저 인증서는 모바일 웹, 앱으로 플러그인 설치없이 복사 지원

## 개인정보보호(개인정보 필터링)

### ■ 사용 목적

- 웹페이지, 게시판, 첨부파일에서 개인정보 노출유무를 점검하여 개인 정보가 외부로 노출되는 것을 사전에 예방해주는 개인 정보 노출 진단

### ■ 대체방안

- 개인정보가 포함된 게시물이 게재 혹은 유입되지 않도록 웹서버에서 콘텐츠 등록 시 차단하는 방식으로 전환·개발

## 브라우저 userAgent

### ■ 사용 목적

- 웹서비스에 접속하는 브라우저의 HTML5 지원 여부를 확인하기 위해서는 자바 스크립트의 navigator객체의 userAgent 문자열을 구분하여 HTML5 지원 브라우저의 경우 플러그인 없는 웹서비스나 이용자 선택 설치 방식을 제공하고, 하위 브라우저(IE8~10)의 경우 기존과 같이 플러그인 설치 방식 제공

### ■ 제공방안

#### 🔗 navigator 객체를 통한 브라우저 정보확인

```
<script>
  var uaString = window.navigator.userAgent;
  if(console && console.log)
    console.log(uaString);
  else
    alert(uaString);
</script>
```

〈표 14〉 브라우저 문자열 구분

브라우저	userAgent값(PC OS)	비고
Internet Explorer	Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko	IE 버전별 체크 필요
Edge	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063	Edge에 Chrome, Safari 문구 포함되어 있어 IE 다음 체크해야 함
Google Chrome	Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36	
Safari (Mac)	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7	
Firefox	Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0	
Opera	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36 OPR/52.0.2871.99	
웨일	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.49 Whale/0.5.12.4 Safari/537.36	

- 브라우저별 userAgent를 구분할 경우 점유율에 따라 IE → Edge → 크롬 → 사파리 →파이어폭스 →오페라 순으로 구분
- 웹과 모바일 웹을 동시에 지원하는 반응형 웹서비스의 경우 모바일 웹브라우저 userAgent와 해상도 확인 후 지원
- userAgent는 브라우저 구분을 위한 용도 이외에도 유입자 이용 통계를 위해 사용하는 경우도 있어, 현재 사용 여부 확인 후 적용 여부 결정 필요

💡 개발 참조(userAgent를 이용한 브라우저 체크)  
 “<https://m.blog.naver.com/vip125/2204467248141>”

# IV

## 부록

1. 자주 묻는 질문(FAQ)
2. 표 목차
3. 그림 목차
4. 용어 설명
5. 약어
6. 참고 문헌

## 1 자주 묻는 질문(FAQ)

### 공인인증서

**문1** 브라우저 인증서는 무엇인가요?

**답1** 웹표준(HTML5)을 지원하는 브라우저의 로컬 스토리지 영역에 인증서를 저장하여 사용하는 방식으로, 별도의 플러그인 없이 본인확인이나 전자서명 기능을 이용할 수 있습니다.

**문2** 공인인증서를 사용하기 위한 플러그인과 브라우저 인증서 모두 지원해야 하나요?

**답2** HTML5 기술 규격을 지원하지 않는 하위 브라우저(IE 8,9,10)는 기존과 같이 플러그인을 통한 전자서명/본인확인 기능을 제공해야 합니다. 브라우저 인증서 지원 브라우저는 아래와 같습니다.

구분		브라우저 인증서 이용 환경
모바일	PC (윈도우7 이상, 맥OS)	MS IE 11 이상, Edge 12 이상, Chrome, Firefox, Safari, Opera
	안드로이드	Android 5.0이상 기본 브라우저, Chrome
	iOS	iOS8.0 이상 Safari, Chrome

**문3** 공동저장소는 무엇이고 반드시 규격을 적용해야 하나요?

**답3** 금융결제원의 공동저장소는 한번 발급으로 여러 운영기관과 인증서를 복사하여 편리하게 전자서명을 사용할 수 있는 기술 규격으로 이용편의성을 위해 적용을 권장합니다. ('18년 11월 서비스 예정)

**문4** 브라우저 인증서 솔루션은 어떻게 도입해야 하나요?

**답4** 기존 공인인증서 플러그인 솔루션 공급업체를 통해 브라우저 인증서 개발 가능 여부 확인(금융결제원 공동저장소 규격 적용 필요)후 도입하는 방식과 브라우저 인증서 솔루션 업체를 통해 도입하는 방안이 있습니다.

문5

브라우저 인증서 도입 시 발생할 수 있는 이슈사항과 해결방법을 자세히 기술해 주세요.

답5

브라우저 인증서는 이용자가 브라우저 캐시 삭제 시 인증서가 같이 삭제되는 불편사항이 있습니다. 이를 개선하기 위해 브라우저 인증서 삭제 시 복구할 수 있는 금융결제원의 공동저장소 기능 도입을 통해 이용 불편을 해결할 수 있습니다.('18년 11월 서비스 예정)

또한 웹사이트별 브라우저 인증서 공동사용을 위해서도 공동저장소 사용을 권장합니다.

### 백신, 개인방화벽, 키보드보안

문6

백신, 개인방화벽, 키보드 보안의 경우 [이용자선택]설치로 안내 되어있는데 플러그인 설치없이 서비스 이용이 가능하나요?

답6

예, 서비스 이용이 가능합니다.

운영기관은 내부 정책에 따라 이용자에게 OS 기본 백신이나 무료(상용) 백신 사용을 권장할 수 있습니다.

### 조회화면 보호(웹 DRM)

문7

상용 웹 DRM 솔루션 제품을 설치하여 사용하고 있으나, 웹표준 자바스크립트 이벤트 제어로 변경하고자 할 때 참고할 수 있는 자료가 있나요?

답7

운영기관은 대민용 서비스 내에 조회화면 보호 기능에 대한 효용성과 필요성을 재검토하여 꼭 필요한 경우에만 적용을 권장합니다.

가이드라인의 “조회화면 보호” 대체 기술에 자바스크립트를 이용한 마우스, 키 이벤트 제어 관련 예제 소스를 이용할 수 있습니다.

이외에도 웹표준으로 조회화면 보호를 지원하는 자바스크립트와 서버 연동 기반 상용 솔루션을 통해서도 조회화면이나 전자문서를 보호할 수 있습니다.

### 전자 결제

문8

PG(Payment Gateway) 사업자의 결제 시스템을 사용하는데, PG가 플러그인을 사용해서 운영기관이 제거할 수 없습니다. 어떻게 제거해야 하나요.

답8

일부 카드결제, 계좌이체 PG는 결제 모듈을 사용할 때 플러그인을 설치합니다. 플러그인 없는 결제를 위해서는 키인 방식 수기 카드결제 방식 개발, 간편수기결제 PG 도입, 간편카드결제 PG로 교체, 간편계좌이체 PG로 교체와 같이 플러그인 없이 결제가 가능한 솔루션을 선택(계약)하셔야 합니다.

## 문서 뷰어

문9

웹폼뷰어와 PDF 내장 뷰어의 구현방식의 차이가 무엇인가요?

답9

웹폼(이폼)뷰어는 HTML5 웹표준으로 전자 증명서 서식을 구현한 웹페이지입니다. 종이 문서와 동일한 형태의 서식을 제공하는 전자서식 솔루션입니다. PDF 내장뷰어는 웹이나 XML서식을 서버에서 PDF로 변환하고, 브라우저에서 기본으로 제공하는 PDF뷰어를 이용하는 방법입니다. 웹폼뷰어와 달리 PDF에는 전자서명, 시점확인 및 보안 기능을 추가할 수 있습니다. 또한 웹폼뷰어 형식의 문서도 PDF로 변환할 수 있습니다.

문10

웹폼뷰어 출력 시 위변조 방지(2D바코드, 복사방지마크, 전자관인) 기능을 제공할 수 있나요?

답10

기존 위변조 방지 플러그인 솔루션은 PDF 파일을 전달받아 PDF 기술표준에 따라 이미지 형태의 2D바코드나 복사방지마크를 합성하는 방식으로 제공합니다. PDF가 아닌 웹폼뷰어는 웹폼을 PDF로 변환 후 위변조 방지 기능을 지원합니다. 이와 별도로 웹폼 문서는 문서확인번호를 문서에 기재하는 방법으로 위변조 방지 기능 제공이 가능합니다.

## 위변조 방지

문11

전자문서(증명서) 위변조 방지를 위한 플러그인 제거(대체) 방안이 있나요?

답11

기존 플러그인에서 제공한 기능과 동일한 기능(2D바코드, 복사방지마크, 워터마크, 전자관인 등)을 서버에서 제공하는 방식으로 구현할 수 있습니다. 다만, 증명서 접수기관에서의 2D 바코드 실제 사용현황, 복사방지마크의 효과성 등을 검토하여 기존 위변조방지 기능을 제거하고, 증명서의 진위확인번호 기재를 통한 진위확인방식으로 대체하는 것을 권장합니다. 또한, 서버에서 제공하는 위변조 방지 기능은 기존 플러그인사용 방식보다 서버 부하가 증가하여 서비스 응답시간 지연 가능성이 존재합니다.

## E-Book 솔루션

문12

전자책 뷰어 플러그인(서고, 뷰어)을 외부 솔루션을 이용해서 제공하고 있는데 어떻게 플러그인을 제거해야 하나요?

**답12** PC용 전자책(EPUB) 뷰어와 서고 시스템은 불법복제를 방지하는 DRM 탑재로 인해 플러그인 형태로 제공하고 있으며, 민간 서비스의 경우 플러그인 제거에 대한 대응이 어려운 점이 사실입니다.  
향후 신규, 재계약으로 PC용 전자책 뷰어 도입 시 플러그인을 지원하지 않는 웹표준 EPUB, PDF 방식으로 제공하는 뷰어, 서고 솔루션을 우선 도입해야 합니다.

## 플러그인 일반

**문13** 플러그인 기술에 대해서 참고할 수 있는 사이트 및 기술 서적에 대해서 알려 주시면 도움이 될 것 같습니다.

**답13** 본 가이드라인의 “II.플러그인 현황 분석“에 대한 설명과 한국인터넷진흥원의 koreahtml5.kr 사이트의 플러그인 기술 소개 및 자료실에 "인터넷 이용환경 개선 기술 안내서"를 참고하실 수 있습니다.

**문14** 개발자 도구를 열지 못하도록 막는 기능(소스보기 금지)을 위한 플러그인을 사용하는데 웹표준으로 해결 방안이 있는지요?

**답14** 웹표준으로 키보드나 마우스 이벤트를 제어할 수는 있으나 개발자도구를 열지 못하도록 제어하는 기능은 웹표준으로 제공할 수 없습니다. 사용자가 개발자도구를 여는 목적은 웹페이지 코드 변경을 통해 입력 값이나 조회 값을 위변조할 목적입니다. 이에 대한 대응 방법으로 클라이언트와 서버 개발 코드에 유효성을 검증하는 코드를 적용할 수 있습니다. 클라이언트 측 검증 코드는 언제든지 회피할 수 있어, 반드시 서버에서 미리 설정된 값 범위와 형식에 대한 유효성을 검증하는 것이 안전합니다.

**문15** 현재 IE 전용 웹서비스를 제공하고 있습니다. 크롬, 사파리, 파이어폭스와 같은 HTML5를 지원하는 브라우저 호환성을 지원하기 위한 방법은 무엇인지요?

**답15** IE8~11만 지원했던 웹서비스의 경우 웹페이지에 브라우저 userAgent 구분을 통한 브라우저별 분기가 되어 있지 않아 플러그인 이용자 선택 설치 화면 제공시 userAgent 구분을 통해 브라우저명, 버전을 확인하는 자바스크립트 코드를 추가해야 합니다. 참고로 ActiveX를 EXE로 전환한 웹서비스의 경우 대부분 브라우저 userAgent로 브라우저 별로 구분되어 있습니다.

## 2 표 목차

표 1_대민용 웹서비스 이용 절차에 따른 플러그인 사용	8
표 2_HTML5 주요 기능 설명	16
표 3_본인인증 또는 실명인증을 위한 방법	22
표 4_본인확인 수단 별 현황	23
표 5_디지털 원패스 본인확인 및 로그인 수단	29
표 6_전자인증서 주요 내용	31
표 7_브라우저 인증서 종류	33
표 8_브라우저 인증서 지원 브라우저 현황	36
표 9_전자문서 시점 확인 기능 및 현황	55
표 10_웹 DRM 웹표준 전환 방안	57
표 11_위변조 방지 및 출력제어 상세 설명	70
표 12_Canvas와 SVG 기능 비교	81
표 13_Canvas 및 SVG 라이브러리	82
표 14_브라우저 문자열 구분	86

그림 1_HTML5 관련 기술 표준 규격(출처 : W3C)	15
그림 2_현재 플러그인 사용 목적별 설치 현황(AS_IS)	19
그림 3_주요 플러그인 사용 목적별 제거 방안(TO_BE)	19
그림 4_회원 가입 유형 및 본인확인 후 가입 절차(출처 : 잡월드 가입화면)	21
그림 5_다양한 본인확인 선택 화면(출처 : 홈택스)	23
그림 6_휴대폰 본인확인 서비스 FLOW	24
그림 7_휴대폰 본인확인 서비스 예시	25
그림 8_신용카드 방식 본인확인 서비스 FLOW	26
그림 9_비회원 카드 본인확인 및 성인인증(출처 : 옥션)	27
그림 10_디지털 원패스 서비스 개념도	28
그림 11_디지털 원패스 도입 기관 적용 절차(출처 : 행정안전부 자료)	28
그림 12_경찰청 스마트 국민제보 디지털 원패스 적용 화면	30
그림 13_금융결제원 공동저장소 개념도	34
그림 14_브라우저 인증서 솔루션 구성	34
그림 15_브라우저 인증서 서비스 제공 화면(출처: 홈택스, 국민은행)	37
그림 16_카드사 수기특약(키인 방식) 가맹 프로세스	40
그림 17_간편수기결제 가맹 프로세스	41
그림 18_카드결제 수기특약에 따른 결제 서비스화면(출처 : KTX)	41
그림 19_간편카드결제 방식 예시(출처 : 페이코)	42
그림 20_간편카드결제 예시(출처 : 네이버페이)	43
그림 21_계좌간편결제 이용 절차(웹, 모바일 웹 지원)	44
그림 22_계좌간편결제 가맹 프로세스	44
그림 23_계좌간편결제 방식 예시(출처 : 네이버페이)	45
그림 24_PC보안 및 공인인증서 플러그인 유형	46
그림 25_플러그인 사용 안내 및 설치 동의 화면 가상 예시	49
그림 26_PC 가상키패드 주요 흐름	50
그림 27_가상키보드 적용 사례(출처 : 홈택스)	50
그림 28_G-SSL 적용 인증서 브라우저 표시 확인(출처 : 경찰청)	52
그림 29_크롬 웹 주소창 SSL 인증서 적용화면(출처 : 홈택스)	54

그림 30_스크린 워터마크 적용 전후	59
그림 31_개발자 도구를 통한 입력 값 변조 예시	60
그림 32_웹폼 서비스 프로세스	62
그림 33_웹폼 문서뷰어 적용 화면 예시	63
그림 34_증명서 조회 순차 적용 화면(출처 : 홈택스)	64
그림 35_부동산 임대차 전자계약서 웹폼 화면(출처 : 국토교통부)	64
그림 36_서버 기반 PDF 변환 및 내장 PDF 연동 예시(출처 : 정보공개포털)	66
그림 37_전자문서진본확인시스템(GTSA) 서버 연동 지원(출처 : 행정안전부)	67
그림 38_연말정산 간소화 PDF 파일 시점 확인 적용 예시	68
그림 39_4대보험 완납 증명서 출력문서 위변조 방지 예시	69
그림 40_플러그인 무설치 전자문서 위변조 시스템	70
그림 41_서버기반 위변조 방지(출처 : 교보생명)	72
그림 42_문서확인번호 단일 기재 방식	73
그림 43_발급번호+문서확인번호 이중 기재 방식	74
그림 44_발급일자+증명서 발급번호 방식	74
그림 45_캡차 적용 발급 문서 진위 확인서비스	74
그림 46_민원24 온라인 발급 문서진위확인 서비스 예시	75
그림 47_출력 가능 프린터 리스트 제어 플러그인	76
그림 48_크롬 브라우저 내장 PDF 뷰어를 통한 전자문서 출력	77
그림 49_HTML5 멀티미디어 기능 요소 별 브라우저 지원 내역	79
그림 50_video.js의 비디오 재생기	80

## 4 용어 설명

### ■ 공인인증서

인증서란, 서명이나 인감도장과 같은 역할을 하는 전자서명이 특정인에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 전자적 정보를 말하며, 공인인증기관이 발급하는 인증서를 공인인증서라 하며, 공인인증서는 비대면 전자서명 용도로만 사용해야하나 구성요소의 소유자 식별정보를 활용하여 본인확인 용도로 과도하게 사용하고 있다.

### ■ 시점확인(TS, Time Stamp)

어느 시점에 데이터가 존재했다는 사실과 그 시간 이후 내용이 변경되지 않았음을 증명하기 위하여 특정 위치에 표시하는 시각. 공통적으로 참고하는 시각에 대해 시간의 기점을 표시하는 시간 변위 매개 변수이다.

### ■ 샌드박스

외부 접근 및 영향을 차단하여 제한된 영역 내에서만 프로그램을 동작시키는 것으로, 샌드박스 내에서 어떤 파일이나 프로세스가 안전하지 못하다고 판명되면, 외부로의 접근을 차단하여 시스템에 피해를 입히는 것을 방지한다.

### ■ 애플리케이션 프로그래밍 인터페이스(Application Programming Interface)

애플리케이션 프로그램에서 사용할 수 있도록, 운영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스이다. 주로 파일 제어, 화면 제어, 데이터 처리, 문자 제어 등을 위한 인터페이스를 제공한다.

### ■ 사용자 에이전트(User-agent)

HTTP 요청 시 HTTP 헤더에 넣어 전송하는 문자열로 브라우저에서는 브라우저 이름, 버전정보 등이 포함된다. 각 브라우저, 검색로봇 마다 다른 문자열이 포함된다.

### ■ 웹애플리케이션(Web Application)

자바스크립트(JavaScript), HTML, CSS등 Web 기반 언어로 개발된 응용 프로그램에서 클라이언트로 웹브라우저나 웹 런타임을 사용하는 모든 응용 프로그램이다.

### ■ 자바스크립트(Javascript)

브라우저에서 실행하는 스크립트 언어를 기술한다. 언어 규격은 자바의 부분 집합(subset)으로 되어 있다. 하이퍼텍스트 생성 언어(HTML) 문서를 작성하는 수준의 이용자가 사용하는 것을 주안점으로 하여 자바의 언어 규격으로부터 변수의 형(정수형이나 문자열형 등)을 생략하거나 새로운 클래스 정의를 할 수 없도록 하였다. 스크립트는 HTML 문서 속에 직접 기술하며, 'script'라는 꼬리표를 사용한다.

## ■ 전자서명

서명자를 확인하고 서명자가 문서에 서명하였음을 나타내기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보이다.

## ■ 플러그인

브라우저가 제공하지 않는 기능을 사용하기 위해 피시(PC)에 설치하고 브라우저와 연동하여 사용하는 별도의 소프트웨어

## ■ 하이퍼텍스트 전송 규약(HTTP)

인터넷의 월드 와이드 웹(WWW) 서버와 WWW 브라우저가 파일 등의 정보를 송수신하는 데 사용되는 클라이언트/서버 규약. WWW 브라우저의 화면상에서 URL(Uniform Resource Locator)를 지정하는 데 사용된다. 예를 들면 'http://www.snu.ac.kr/index.html'과 같이 'http://'로 시작되는 URL을 지정하면, 여기에 있는 데이터를 하이퍼텍스트 전송 규약(HTTP)을 사용하여 서버에서 브라우저로 전송한다.

## ■ 캡차(CAPTCHA)

봇에 의한 자동 입력인지 사람이 입력하는 지를 식별하기 위한 방법. 임의의 숫자나 문자를 컴퓨터가 알아보기 어렵게 하여 표시한 후 이에 대한 값을 입력하도록 요청하는 방식. 때로는 사람도 알아보기 어렵다.

## ■ CSS3(Cascading Style Sheets3)

웹 문서의 전반적인 스타일을 미리 저장해 두는 기술로 CSS3의 경우 그림자 효과, 그라데이션, 변형 등 그래픽 편집 프로그램으로 제작한 이미지를 대체할 수 있는 기능과 다양한 애니메이션 기능이 추가되어 CANVAS, SVG, WebGL과 함께 어도비 플래시를 대체하고 있다.

## ■ HTML5(HyperText Markup Language 5)

HTML의 완전한 5번째 버전으로 월드 와이드 웹 (World Wide Web)의 핵심 마크업 언어로 비디오, 오디오 등 다양한 부가기능과 최신 멀티미디어 콘텐츠를 액티브X 없이 브라우저에서 쉽게 볼 수 있게 하는 것을 목적으로 한다. 2014년 10월 28일 HTML5 표준안을 확정했으며, 현재는 2017년 12월14일에 제정한 HTML5.2 표준안을 준수하고 있다.

## ■ PDF (Portable Document Format)

원본 문서가 어떠한 애플리케이션에서 작성되었는지에 상관없이 여러 플랫폼 환경에서 문서를 동일하게 출력하고 디스플레이 할 수 있도록 해주는 파일 포맷. 미국 어도비사가 개발하여 전자 문서의 사실상 표준(de facto standard)으로 자리 잡아 오다가 2008년 국제 표준화 기구 국제 표준(ISO 32000-1)으로 채택되었다.

API	Application Program Interface
ARS	Advanced Record System
CORS	Cross-Origin Resource Sharing
CMP	Certificate Management Protocol
CMS	Content Management System
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service attack
DNS	Domain Name System
E2E	End to End
ECMA	European Computer Manufacturers Association
EPUB	Electronic Publication
EME	Encrypted Media Extensions
FDS	Fraud Detection System
GTSA	Government Time Stamp Authority
G-SSL	Government Secure Socket Layer
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
HSM	Hardware security module
ISP	Internet Secure Payment
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
MPEG	Moving Picture Experts Group
NPAPI	Netscape Plugin Application Programming Interface
OTP	OneTime Password
OS	Operating System
PKI	Public Key Infrastructure
PDF	Portable Document Format
PG	Payment Gateway
RDP	Remote Desktop Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
SOP	Same-Origin Policy
SSL	Secure Socket Layer
SVG	Scalable Vector Graphics
VPN	Virtual Private Network
W3C	World Wide Web Consortium
XML	Extensible Markup Language

## 공인인증서/브라우저 인증서

- “웹 표준 기반 공인인증서비스 도입 및 구현 기술 안내서”(한국인터넷진흥원, 2014)
- “간편 공인인증서 인터페이스 가이드라인”(한국인터넷진흥원, 2016)
- W3C Web Cryptography API  
<https://www.w3.org/TR/WebCryptoAPI/>
- "브라우저 인증서비스 가이드라인"(금융결제원, 2018)
- “브라우저인증서 공동저장소 개발자 매뉴얼”(금융결제원, 2018)
- 행정전자서명 인증관리센터  
<https://www.gpki.go.kr/main/PreMainAction.action>
- Web Storage (Second Edition)  
<https://www.w3.org/TR/webstorage/>

## 웹 표준

- “HTML5 웹애플리케이션 개발 지침“안내서”(KCS, 2014)
- W3C HTML5.1 표준 기술  
<https://www.w3.org/TR/html51/>
- 공개 웹 프레임워크와 라이브러리 기술 자료  
<http://webframeworks.kr>
- 브라우저 별 HTML5 지원 확인  
<http://caniuse.com/>  
<https://html5test.com/>
- 브라우저 userAgent 확인  
<http://www.useragentstring.com/>

## 보안

- HTML5 암호기술 이용 안내서(한국인터넷진흥원, 2018)
- 보안서버구축 안내서(한국인터넷진흥원, 2009)
- 보안서버 구축 가이드(과학기술정통부, 2013)
- 전자정부 웹서비스 인증서(G-SSL) 구축가이드 7.0(행정안전부, 2017)

- 홈페이지 취약점 진단·제거 가이드(기술안내서)  
<http://www.kisa.or.kr/public/laws/laws3.jsp>
- HTML5 Security Cheat Sheet  
[https://www.owasp.org/index.php/HTML5\\_Security\\_Cheat\\_Sheet](https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet)
- “홈페이지 SW(웹) 개발보안 가이드” (행정안전부, 2012)
- “W3C의 웹보안 동향과 HTTPS 구축 지침” (HTML5융합기술포럼, 2017)
- 조희화면보호 JQuery 소스  
<http://blog.work6.kr/10>
- 서버 유효성 검증 예시  
<https://jojoldu.tistory.com/129>

### 전자문서

- jsPDF / pdf.js  
<https://github.com/MrRio/jsPDF>  
<https://www.mozillalabs.com/pdfjs/>
- “전자문서 진본확인 서비스 연계 기술규격”(행정안전부, 2017)
- “전자문서에 첨부된 전자서명 육안확인 기술 연구”(한국인터넷진흥원, 2011)

### 플래시 대체

- Chrome의 Flash 차단 정책과 Flash에서 Canvas로 전환 사례  
<https://d2.naver.com/helloworld/1899560>

### 멀티미디어

- HTML5 Video Player 비교  
<http://videosws.praeganz.de/>
- Top 10 Best HTML5 Audio Players  
<http://www.scratchinginfo.net/top-10-best-html5-audio-players>

### 플러그인 대체

- HTML5 기술 지원 센터  
<https://www.koreahtml5.kr/main.do>
- “인터넷이용환경개선을 위한 기술안내서”(한국인터넷진흥원, 2016)