



나라장터종합쇼핑몰

이미지 속 개인정보의 유출 사례 분석과 안전한 개인정보보호

I. 이미지 속 개인정보의 유출 사례 분석

1. 파일 유형 및 노출 사례

표 1 파일 유형 및 노출 사례

파일 유형	노출 사례
엑셀(.xlsx 등)	[숨기기] 기능에 의해 개인정보가 노출
	시트 보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보가 노출
	함수 치환 후 원본 내용 미삭제로 인해 개인정보가 노출
	[메모] 기능으로 개인정보가 노출
	배경색과 같은 글자색으로 개인정보를 작성하여 노출
	OLE(Object Linking and Embedding) 객체 연결로 인한 개인정보 노출
	외부 파일 참조 기능으로 인한 개인정보 노출
문서(.hwp .docx 등)	문서 파일에 개인정보가 노출
이미지(.jpg .png .pdf 등)	이미지 파일에 개인정보가 노출

”

모든 제품이
기능 지원

출처 : 홈페이지 개인정보 노출방지안내서 (2020년 12월)

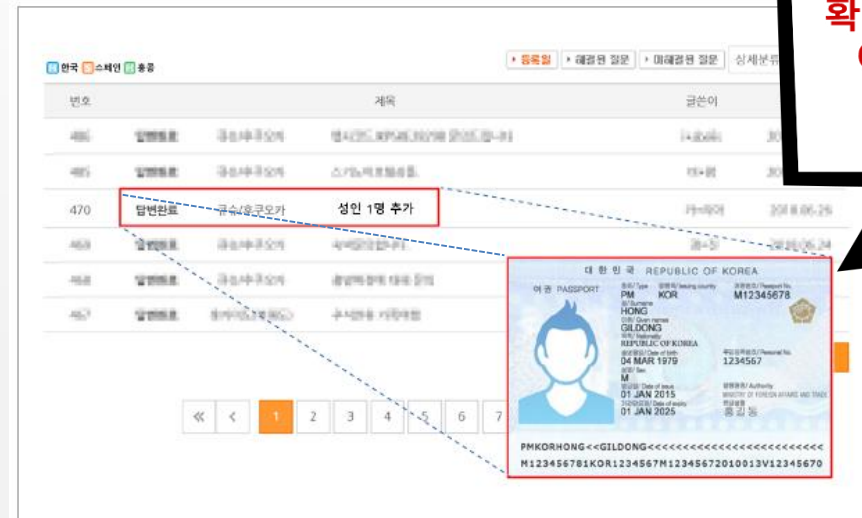
I. 이미지 속 개인정보의 유출 사례 분석

2. 이미지 파일에 대한 노출 사례

노출사례 ③ - 이미지 파일(.jpg .png .pdf 등)을 통한 개인정보 노출

A씨는 B여행사를 통해 항공권과 숙소를 예약했다. A씨는 예약인원 추가를 위해 여권사본(스캔본)을 여행사 담당자에게 메일로 보냈다. 하지만 업무담당자가 예약자 확인을 위해 홈페이지 공개 게시판에 여권사본 이미지 파일을 등록하면서 해당 개인정보(이름, 여권번호, 생년월일 등)가 노출되었다.

그림 14 이미지 파일에 의한 개인정보 노출 사례



항공사에서 예약자
확인을 위해 홈페이지에
여권 이미지 파일을
등록하여 노출 됨

출처 : 홈페이지 개인정보 노출방지안내서 (2020년 12월)

I. 이미지 속 개인정보의 유출 사례 분석

3. 검색엔진을 통한 노출 사례

4. 검색엔진을 통한 개인정보 2차 노출

가. 검색엔진의 이해

검색엔진이란 인터넷 상에서 자료를 쉽게 찾을 수 있도록 검색사이트에 구축된 기능이다. 검색엔진은 정보수집·정보가공·정보제공의 세 가지 기능으로 구성되는데 정보수집은 크롤러, 정보가공은 인덱서, 정보제공은 사용자 인터페이스가 담당한다. 검색엔진의 정보수집 단계에서 크롤러가 인터넷에 있는 웹사이트를 주기적으로 방문하여 각종 정보를 자동으로 수집하는데, 이 때 웹사이트의 일부 웹페이지가 검색엔진 내 일정기간 동안 보관된다. 가령 주민등록번호 등 개인정보를 포함한 웹페이지가 검색엔진에 수집될 경우 원 사이트에서 해당 웹페이지의 개인정보를 삭제 조치하더라도, 크롤러가 개인정보가 삭제 조치된 웹페이지를 재 수집하지 않는 동안 개인정보가 여전히 검색엔진에 검색될 수 있다. 따라서 홈페이지에 개인정보가 잠시라도 업로드 된 경우에는 반드시 해당 노출 내용이 검색엔진에 의해 수집되었는지를 확인하고 검색엔진에 남아 있는 개인정보를 삭제해야 한다.

홈페이지에 등록된
내용이 검색엔진을 통해
노출 됨

출처 : 홈페이지 개인정보 노출방지안내서 (2020년 12월)

I. 이미지 속 개인정보의 유출 사례 분석

3. 검색엔진을 통한 노출 사례

“에어비앤비 이용자 신분증·개인정보 구글에 통째로 노출됐다” - YTN 2018년 10월 22일



여권, 운전자 번호 등은
개인정보라고 생각하지 않아
그대로 노출됨



이미지 속에 개인정보가 많이 포함되어
있는 것을 일반인들은 인식을 못하고
있습니다.
이미지 내의 문자에 대해서도 개인정보
보호가 반드시 필요합니다.

I. 이미지 속 개인정보의 유출 사례 분석

4. 문서 등록시 육안으로 개인정보 포함 여부 확인하라

홈페이지 운영·관리자는 첨부파일 업로드 전에 해당파일 내 개인정보가 존재하는지 확인해야 하며, 공개된 게시판에 첨부파일을 업로드 해야 하는 경우 마스킹 처리 등을 통해 개인정보가 식별되지 않도록 조치해야 한다.

엑셀이나 한글 및 텍스트 기반의 PDF 파일은 검색 기능을 통해 개인정보가 포함되어 있는지 확인 가능하지만 이미지는 검색 기능을 통해 확인이 어려우므로 PDF 파일 생성 전 개인정보 포함 여부를 반드시 육안으로 확인 후, 마스킹 처리하여 PDF 파일로 변환하여야 한다.

그림 15 이미지 마스킹 처리 예시



출처 : 홈페이지 개인정보 노출방지안내서 (2020년 12월)

파일 생성전에
개인정보 포함 여부를
육안으로 확인 하라.



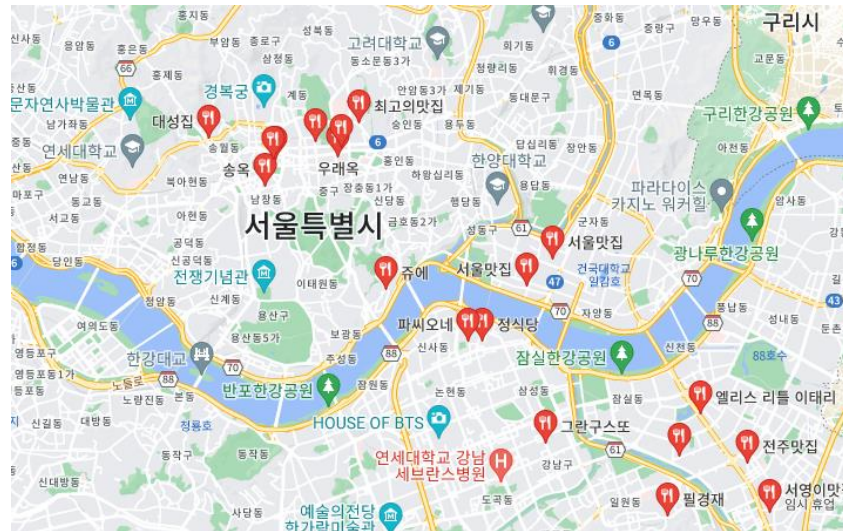
육안으로 개인정보
식별 불가능

I. 이미지 속 개인정보의 유출 사례 분석

5. 개인정보가 있을까? 없을까? (실제 사례임)

☑ 예제 파일명 : 서울시 맛집 검색.ppt

서울시 맛집 지도



I. 이미지 속 개인정보의 유출 사례 분석

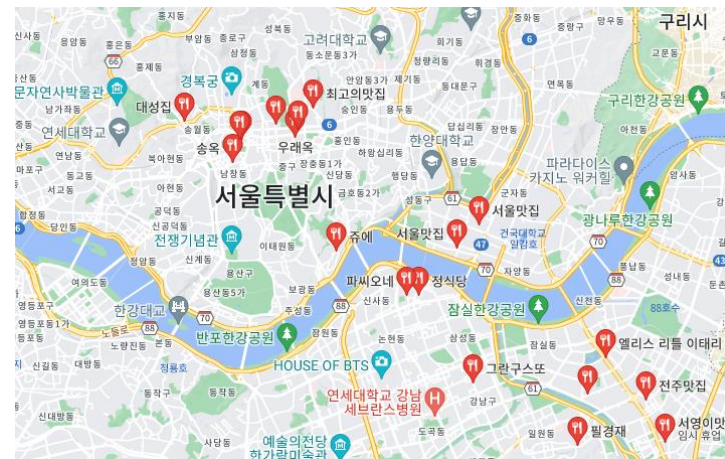
5. 개인정보가 있을까? 없을까? (실제 사례임)

☑ 예제 파일명 : 서울시 맛집 검색.ppt

서울시 맛집 지도

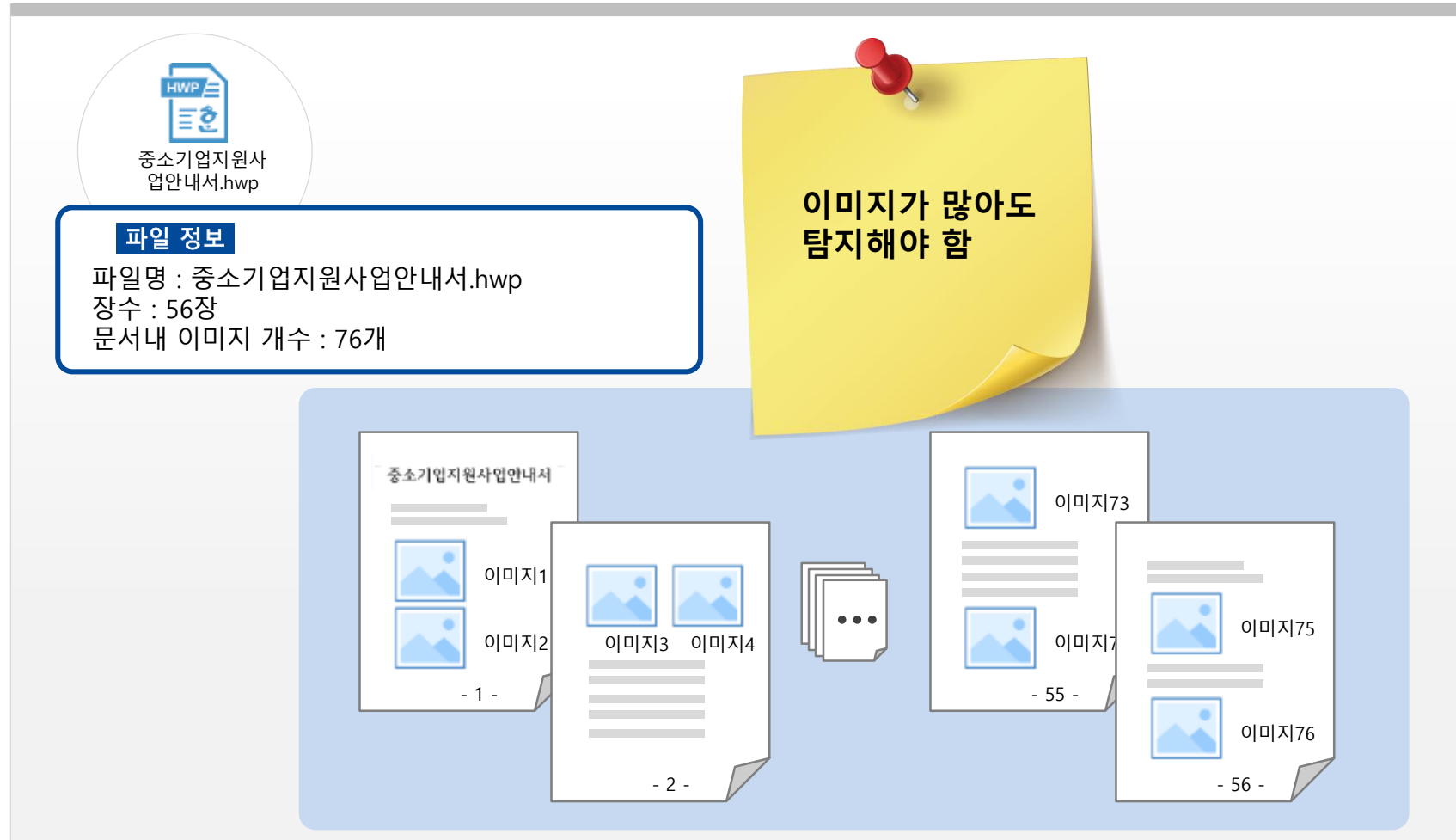


각각의 이미지까지도 모두 분리하여 보면
개인정보가 포함된 이미지가 가려져 있는
경우도 있다.
눈으로는 확인 할 수 없음.



I. 이미지 속 개인정보의 유출 사례 분석

6. 하나의 문서에 이미지가 대량으로 포함되어 있을 경우



I. 이미지 속 개인정보의 유출 사례 분석

7. 개인정보 스캐너로 탐지 했는데도 개인정보를 보유

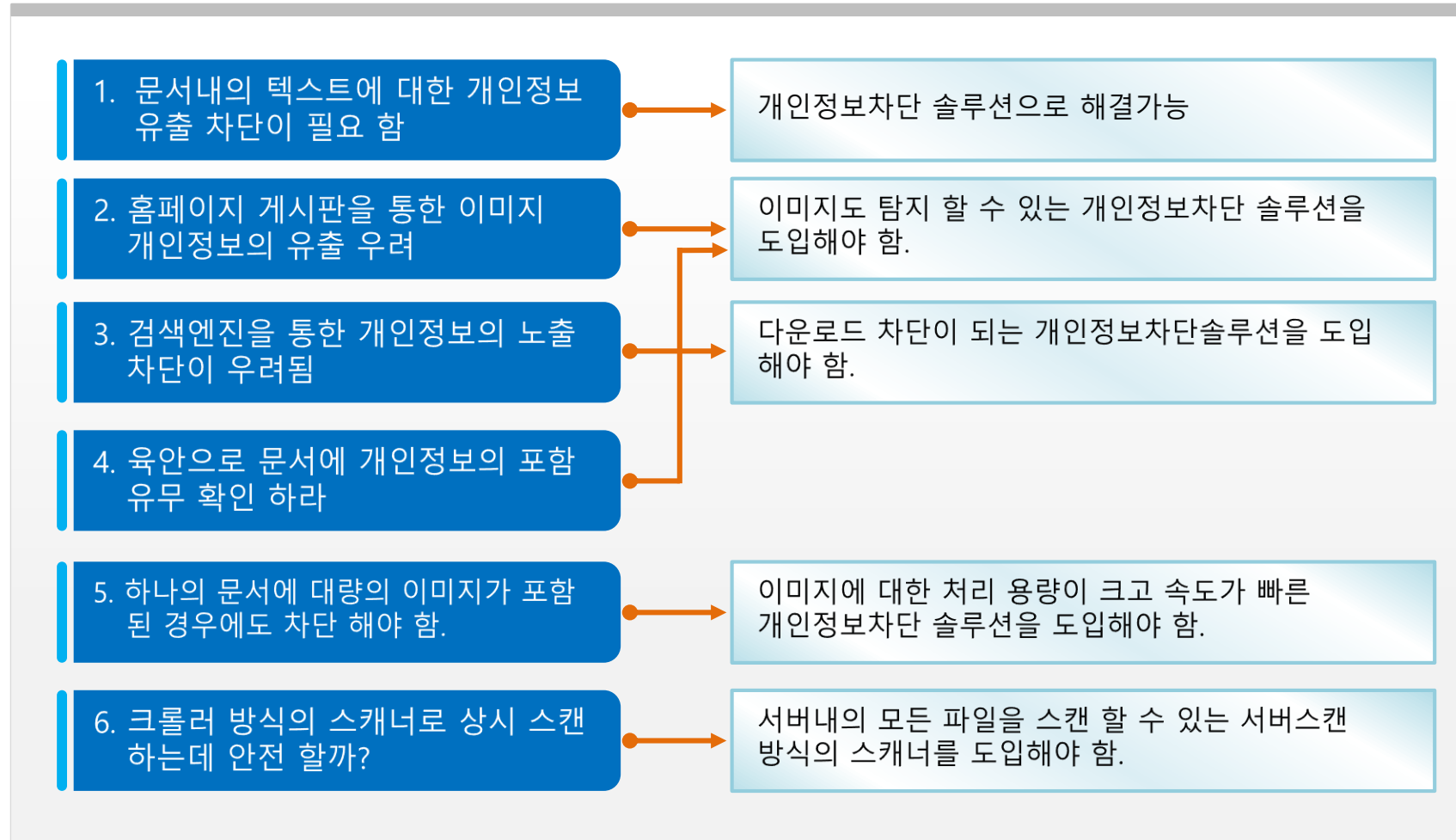
** 구청 : 수시로 크롤링 방식의 개인정보 스캐너로 검색을 했었는데도 링크가 끊어진 파일에서 개인정보 수백건이 나옴.

****원 : 크롤링 방식의 스캐너로 용역서비스를 받고 있었는데 서버스캔 방식으로 스캔 후 이미지 파일과 텍스트에서 개인정보 수십 만건이 나옴.

크롤링 방식의 스캐너 (kisa에서 스캔 하고 있는 방식)는 홈페이지의 링크를 따라가면서 스캔 하는 방식이기에 스캔은 간단 하지만 링크가 끊어진 경우에는 개인정보가 포함된 파일이 있어도 탐지 해 내지 못하는 단점이 있음.

I. 이미지 속 개인정보의 유출 사례 분석

8. 개인정보의 유출 사례 분석 결과



II. 정보보호의 방법

1. 현재까지의 정보보안과 대응방안



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

2. 도면 유출 탐지 솔루션



CAD파일의 확장자 뿐만 아니라 도면 파일을 이미지로 변환하여 유출하는 행위에 대한 차단



다양한 CAD 파일
도면을 이미지로 변환한 파일
JPG, GIF, PNG, TIFF, BMP
PDF 파일에 대한 차단

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션 (ImageOCR & OCR Filtering)



홈페이지 게시판 내의 “이미지”와 “이미지가 포함된 문서파일”에 대해 개인정보를 탐지하고 유출을 차단하는 제품입니다.



적용 대상 개인정보 및 파일 형식

개인식별자

- 주민등록번호
- 외국인등록번호
- 운전자번호
- 여권번호
- 계좌번호
- 이메일 주소
- 신용카드번호
- 건강보험번호
- 기타 개인정보
- 불건전게시물

문서파일 유형

- 이미지(JPG, GIF, PNG, TIFF, BMP 등등)
- 한글, MS오피스, 압축파일, PDF 파일내의 텍스트 및 이미지에 대하여 개인정보를 탐지 및 차단



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션 (전자결재 시스템 포함)



이미지 속 개인정보를 차단 할 수 있는 OCR 모듈이 탑재된 개인정보 보호 솔루션이 필수

OCR 모듈의 탑재

- 이미지에서 문자를 추출하여 문서 내의 이미지나 이미지 파일에서 개인정보를 탐지하여 차단 하는 모듈



이미지에 대한 개인 정보 차단

기존의 Filtering 모듈

- 문서 내의 텍스트에 대하여 개인정보를 탐지하고 차단 하는 모듈



텍스트에 대한 개인 정보 차단

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

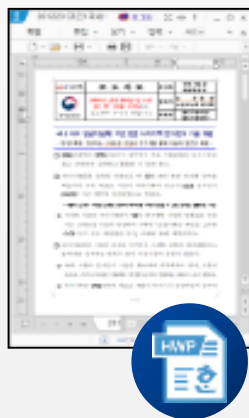
3. 홈페이지 개인정보차단 솔루션 (전자결재 시스템 포함)



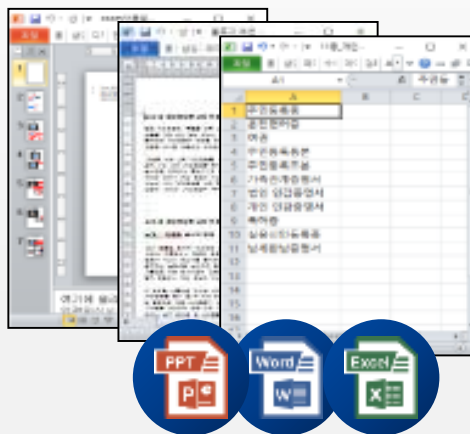
탐지해야 하는 문서

- 1) 문서 내의 텍스트는 물론 문서내의 이미지도 탐지 해야함.

한글문서



MS Office 문서



이미지 파일

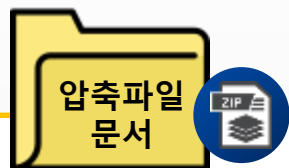


Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

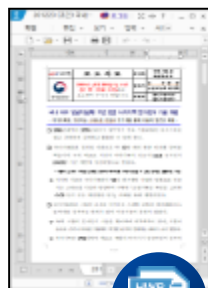
3. 홈페이지 개인정보차단 솔루션 (전자결재 시스템 포함)

 탐지해야 하는 문서

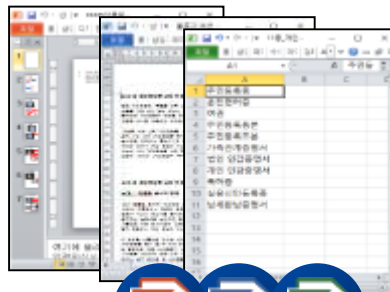
- 1) 문서 내의 텍스트는 물론 문서내의 이미지도 탐지 해야함.



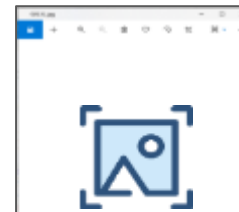
한글문서



MS Office 문서



이미지 파일



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션 (전자결재 시스템 포함)



탐지해야 하는 문서

3) 하나의 문서에 대량의 이미지가 포함된 문서



중소기업지원사업안내서.hwp

파일 정보

파일명 : 중소기업지원사업안내서.hwp

장수 : 56장

문서내 이미지 개수 : 76개



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션 (전자결재 시스템 포함)

업로드 차단

사용자가 게시판에 글을 업로드 할 때 개인정보가 포함되어 있으면 차단이 되며, 문서 내의 텍스트는 물론이고 이미지 속의 개인정보도 차단됨.



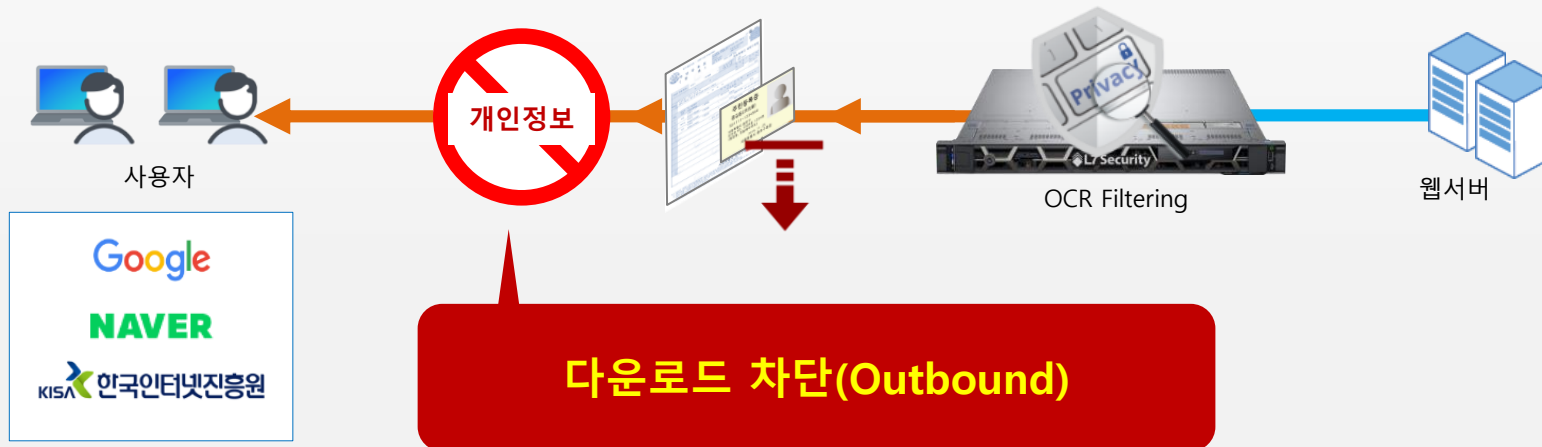
Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션 (전자결재 시스템 포함)



다운로드 차단

- 사용자가 게시판의 글을 클릭하여 다운로드 할 때 개인정보가 포함되어 있으면 차단이 되며, 문서내의 텍스트는 물론이고 이미지 속의 개인정보도 차단됨.
- 구글이나 네이버의 검색엔진이 접근시 개인 정보가 있으면 차단 됨.
- 한국인터넷진흥원에서 개인 정보 스캔시 개인 정보가 있으면 차단 됨.



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션



다운로드 차단

개인 정보의 안전성 확보조치 기준 해설서 (제 6조 접근통제)

- 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 한다.
 - 인터넷 홈페이지의 설계, 개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 인터넷 서비스 검색엔진(구글링 등) 등을 통해 관리자 페이지와 취급중인 개인정보가 노출되지 않도록 필요한 조치를 한다.

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션



다운로드 차단

"개인정보 안전성 확보조치기준 해설서"에 따라 구글이나 네이버 등의 검색 엔진이 접근시 개인정보의 유출을 차단하기 위해서는 반드시 다운로드 차단이 필수적임.

다운로드 차단이 되어야만 완벽한 개인정보 보호법 준수가 가능 함.

개인 정보의 안전성 확보조치 기준 해설서 (제 6조 접근통제)

- 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 한다.
 - 인터넷 홈페이지의 설계, 개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 인터넷 서비스 검색엔진(구글링 등) 등을 통해 관리자 페이지와 취급중인 개인정보가 노출되지 않도록 필요한 조치를 한다.

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

3. 홈페이지 개인정보차단 솔루션

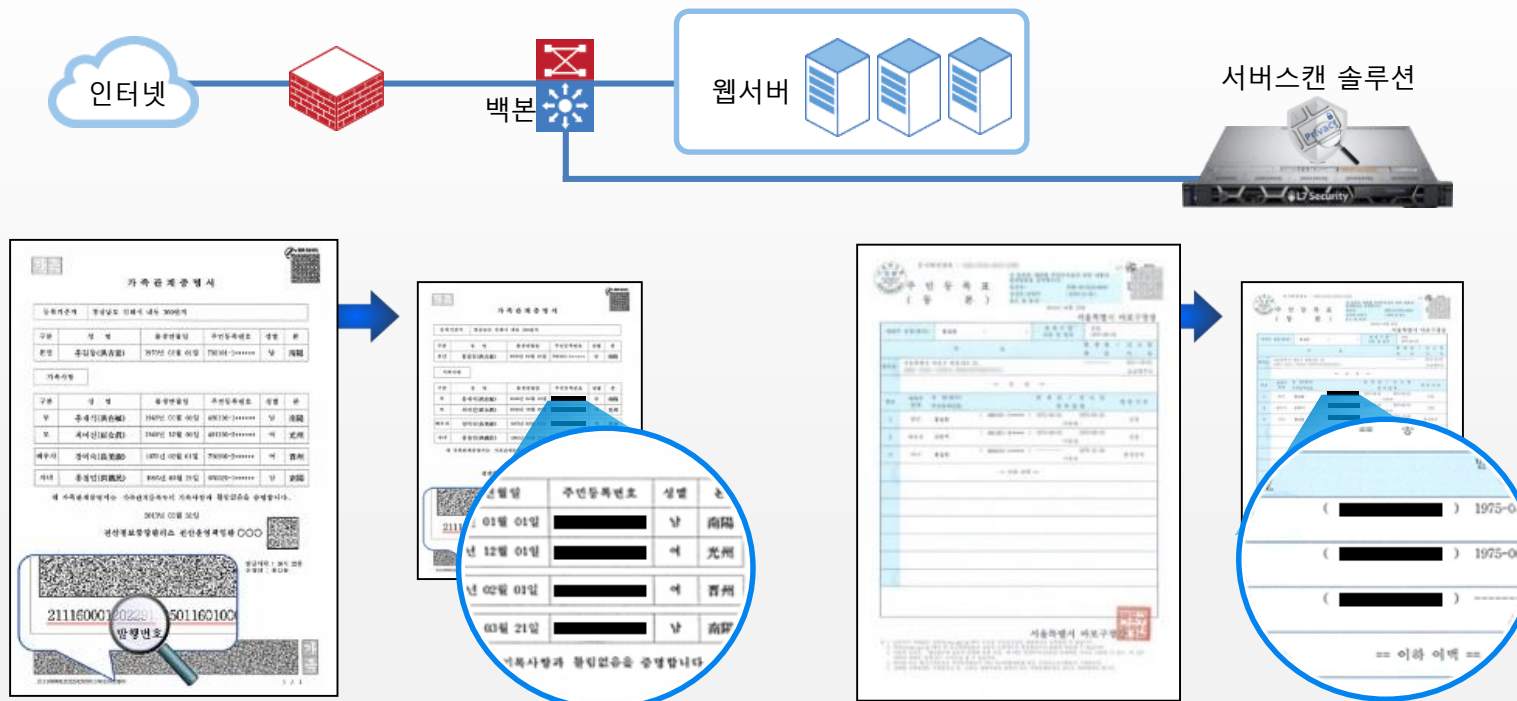
다운로드 차단



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

4. 이미지 파일에 대한 서버스캔 및 마스킹 ImageScanner & Masking

1 문서에서 개인정보가 포함된 부분을 추출하여 마스킹 기능 지원



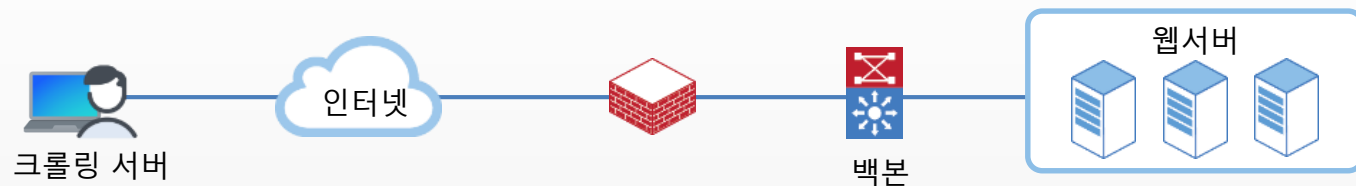
Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

4. 이미지 파일에 대한 서버스캔 및 마스킹 ImageScanner & Masking



개인정보 노출 진단 방법은 크게 두가지가 있습니다. 하나는 크롤러 방식의 진단이고 다른 하나는 서버를 직접 스캔 하는 방식의 진단이 있습니다.

크롤링 방식의 진단



장점

- 기관의 외부에 설치 되기에 기관의 담당자가 설치에 대해 신경쓰지 않아도 된다.

단점

- 웹사이트의 링크를 로봇이 따라가면서 개인정보를 스캔 하는 방식이기에 프로그램 환경에 따라 링크를 못 따라가는 경우가 발생하여 개인정보를 찾아 내지 못하는 경우가 있다.
- 게시판을 스캔 했는데 모든 게시판을 스캔 했는지 담당자는 파악이 불가하다.
- 로그인 방법이 사이트 마다 다르기에 모든 사이트를 스캔 하기가 어렵다

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

4. 이미지 파일에 대한 서버스캔 및 마스킹 ImageScanner & Masking



개인정보 노출 진단 방법은 크게 두가지가 있습니다. 하나는 크롤러 방식의 진단이고 다른 하나는 서버를 직접 스캔 하는 방식의 진단이 있습니다.

서버 스캔방식의 진단

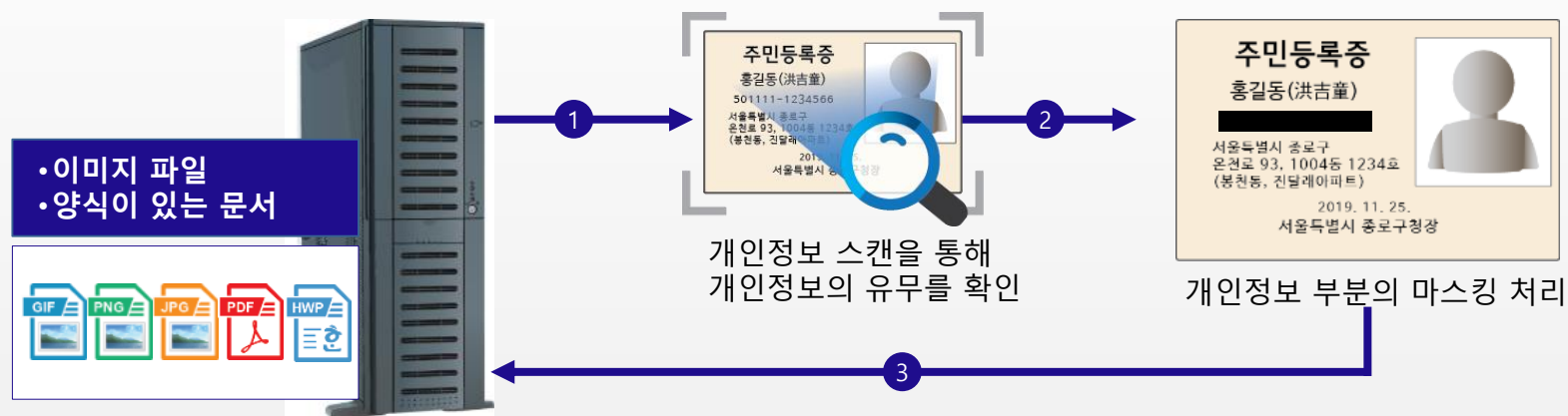


장점	단점
<ul style="list-style-type: none">• 서버내의 모든 파일에 대하여 개인정보를 스캔 하므로 완벽히 탐지를 해 낼 수 있다.• 스캔하여 탐지된 개인정보파일을 마스킹까지 할 수 있다	<ul style="list-style-type: none">• 서버실 내부에 설치 해야 하기에 스캔 할 서버의 접속 ID와 PW를 등록해야 하기에 설치가 번거롭다.

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

4. 이미지 파일에 대한 서버스캔 및 마스킹 ImageScanner & Masking

- 서버 내의 개인정보나 중요정보가 포함된 문서를 찾기 위한 기능으로 문서 내의 텍스트는 물론이고 이미지 속의 개인정보나 중요정보를 찾을 수 있음.
- 탐지된 문서에서 이미지 파일이나 PDF파일 속의 개인정보나 중요정보에 대해 마스킹 처리가 가능함.



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

4. 이미지 파일에 대한 서버스캔 및 마스킹 인증현황

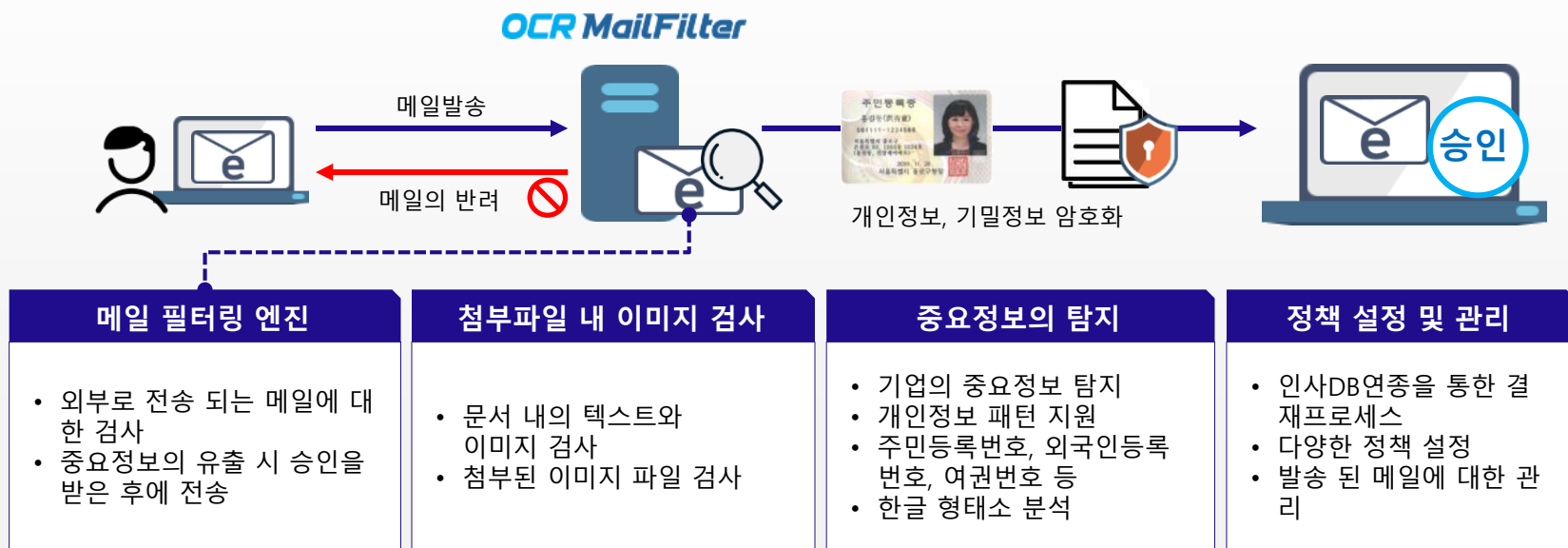


Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

5. 이메일을 통한 정보보호 솔루션 OCR MailFilter



이 이미지를 통한 중요정보와 개인정보의 탐지 방안



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

6. 이미지 문서 디지털화 솔루션

OCR 대상



The image shows a Korean Resident Registration Certificate (주민등록표) with several red boxes highlighting specific information:

- 1. Document Confirmation Number (문서확인번호): 1592-8724-9516-4879
- 2. Resident Registration Certificate (주민등록표)
- 3. Seoul Special City Mapo-gu Office (서울특별시 마포구청장)
- 4. Resident Name (세대주 성명): 홍길동
- 5. Address (주소): 서울특별시 마포월드컵로 212
- 6. Resident Name (본인): 홍길동
- 7. Resident ID Number (주민등록번호): 480101-1234567
- 8. Spouse Name (배우자): 김순이
- 9. Spouse Resident ID Number (배우자 주민등록번호): 491201-2234567
- 10. Child Name (자녀): 홍길순
- 11. Child Resident ID Number (자녀 주민등록번호): 950212-2233456

OCR 결과

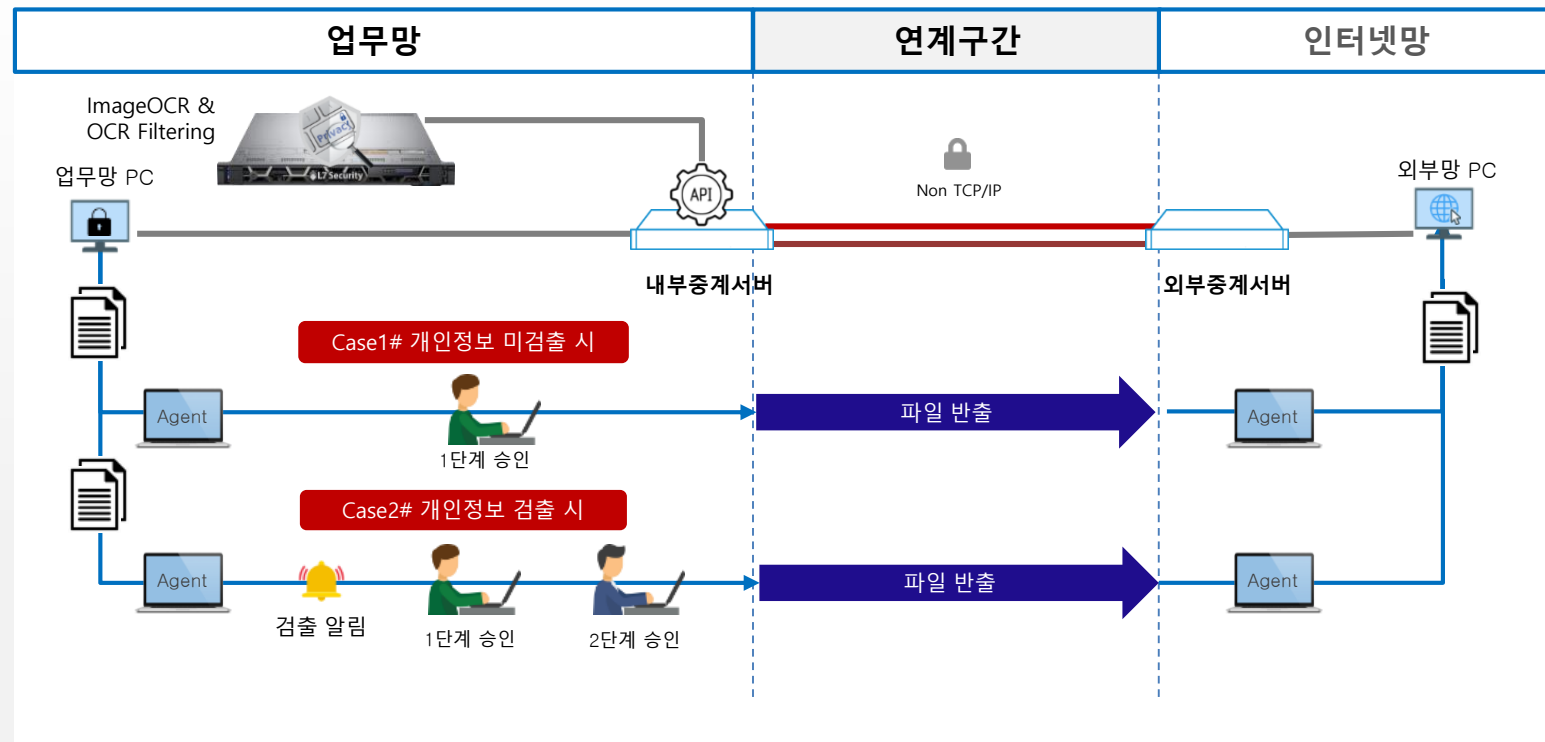
주민등록 등본

① 문서확인번호	1592-8724-9516-4879
② 구분	주민등록표(등본)
③ 발행처	서울특별시 마포구청장
④ 세대주 성명	홍길동
⑤ 주소	서울특별시 마포월드컵로 212
⑥ 본인	홍길동
⑦ 주민등록번호	480101-1234567
⑧ 배우자	김순이
⑨ 주민등록번호	491201-2234567
⑩ 자녀	홍길순
⑪ 주민등록번호	950212-2233456

Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

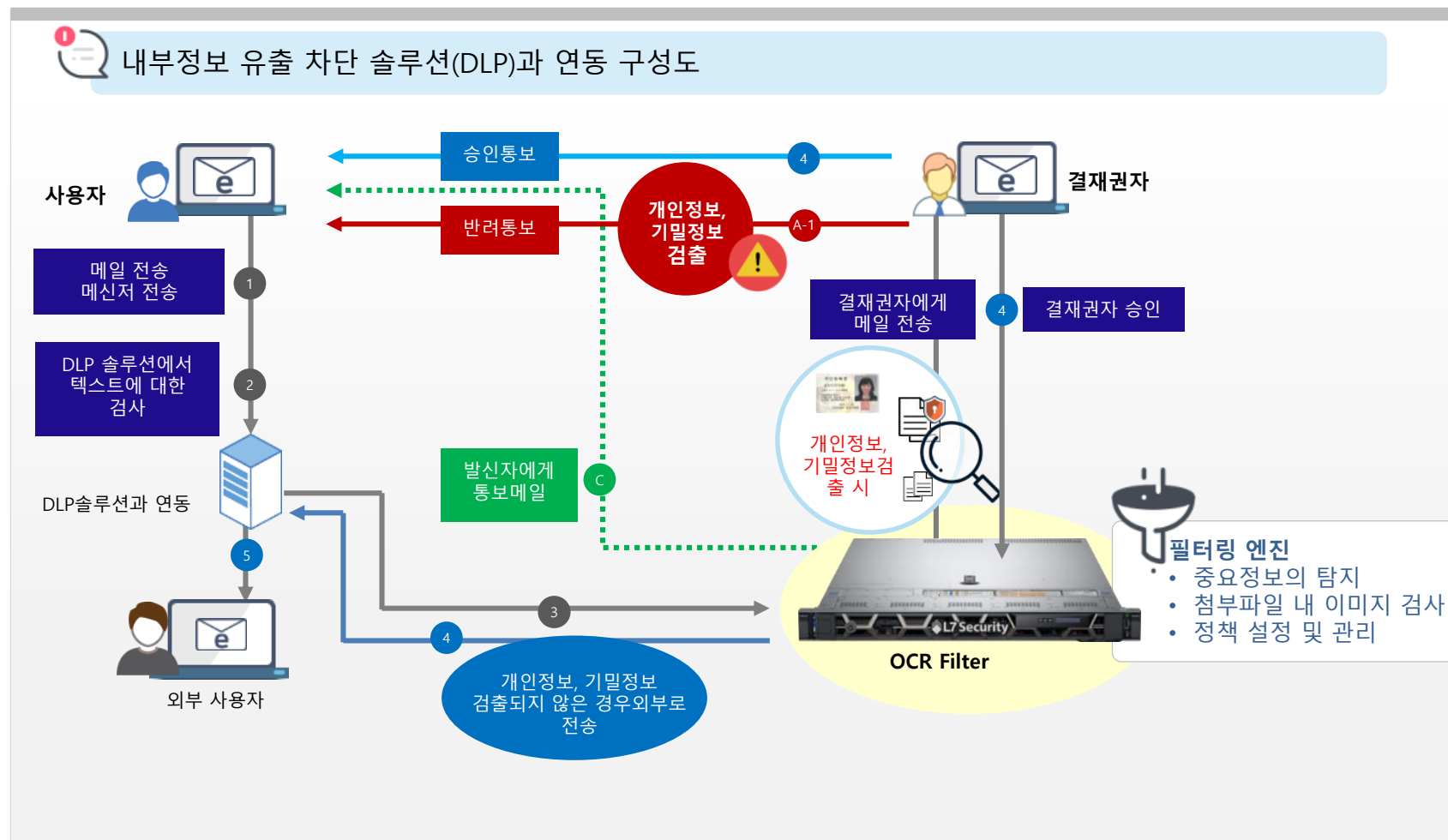
7. 망연계 솔루션과의 연동

망연계시스템과 연동하여 개인정보의 탐지가 가능합니다.



Ⅲ. 이미지 정보보호 기능이 탑재된 솔루션 소개

8. 내부정보유출 차단 솔루션과의 연동



IV. 결론

엘세븐시큐리티는



이미지에서 문자를 추출하는 OCR 모듈을 개발하여 개인정보 보호는 물론이고 업무 효율을 향상 시키는 RPA에 적용하여 새로운 사업분야를 열고 있다.

이미지에서 문자를 추출 하는
OCR 모듈의 개발사로
다양한 제품을 개발하고 있음.

OCR과 네트워크 기술이 결합되어
새로운 분야의 제품 개발로
시장을 리드하고 있음.



OCR의 성능이 우수하여
문자인식율이 높고
문자추출 시간이 빠름

OCR 모듈을 이용하여
RPA에 적용하여 업무효율을
향상 시키는 사업을 시작 함.

V. 이벤트

“ 엘세븐시큐리티에서 기존서버 1~2대에 대한 무상점검 이벤트를 진행 합니다. ”

ImageScan 프로모션 구성

1. 본 솔루션을 직접 사용하기를 원하는 고객 및 파트너사에는 당시 서버와 일체형 Package Demo 장비를 무상으로 지원하여 점검해 드립니다.(Demo 기간 : 1일 ~ 3일)

- 점검 대상서버(1대 기준) : EDMS, WAS 등 감시 대상서버에 자사 Demo 장비를 연결하여 개인정보 보호 조치 필요성 유무 판단
(검출이 안될 경우 대상 서버 변경 가능)



VI. 비대면 제품소개/상담 안내

www.L7secu.com

제품/기술 문의

비대면 제품소개/상담 신청



홈페이지에서 비대면 상담 신청



비대면 제품소개/상담 신청서 작성

제품 소개 및 상담을 신청해주세요.

- 이름 *
- 회사명 *
- 전화번호 *
- E-mail *

■ 문의하시는 회의 날짜와 시간을 선택하시면 최대한 일정을 맞춰서 적합한 상대방을 보내드립니다.

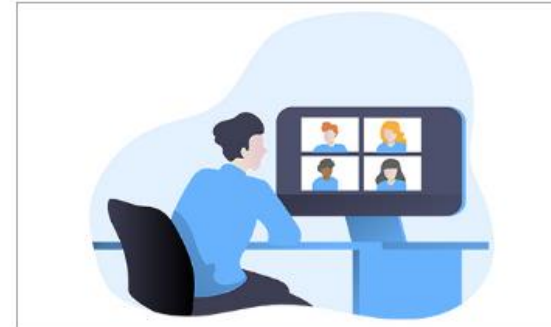
- 회의 날짜 *
- 연도-월 *
- 회의 시작 시간 *
- 시간을 선택하세요 *
- 내용 *

SUBMIT

비대면 상담 초대장을 이메일로 전송



비대면 상담 진행



감사합니다.

 **L7 Security**
(주)엘세븐시큐리티
T. 02-6929-0505
www.L7secu.com

담당자 권영우 부장
T. 010-7234-4673
kwon@L7secu.com