



설록홈즈

(주)컴트루테크놀로지

[보안백서 시리즈]

방치된 DB서버, 파일서버를 위한

서버개인정보

진단레시피



〈클릭〉

서버스캔

무료 체험신청



〈문 의〉

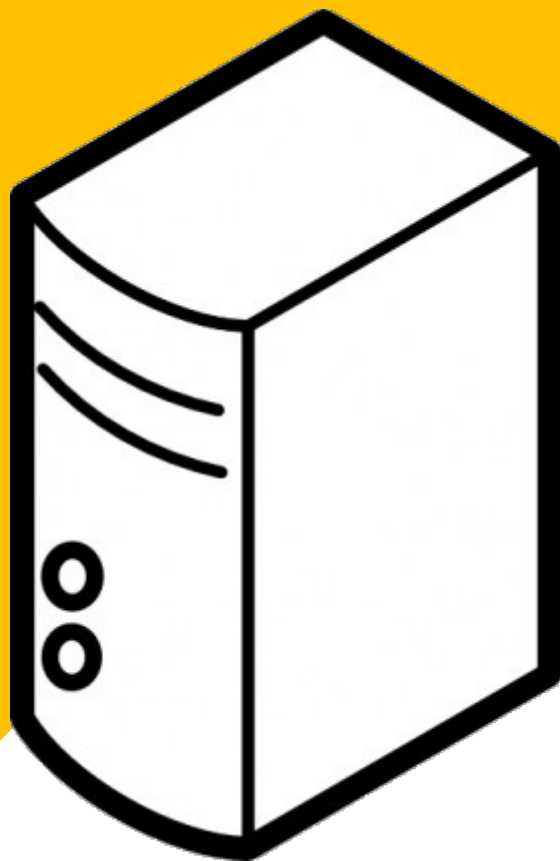
김 현 정 대리 mkt@comtrue.com 02-396-7005(304)

(주)컴트루테크놀로지 서울시 마포구 상암동 1580번지(성암로 330)

DMC 첨단산업센터 4층 전화 : 02-396-7005 이메일: sales@comtrue.com

홈페이지: www.comtrue.com

2015.08.12 기획팀 발간 / 무단전재 및 재배포 금지



COMTRUE[®]
Technologies

목차

1. 서버 개인정보보호와 관련법

1-1. 개인정보보호법

1-2. 정보통신망법

2. 서버 개인정보보호 이슈

2-1. 서버 개인정보보호

2-2. 서버 개인정보보호 STEP

2-3. 서버 개인정보 검출 관리 솔루션

3. 서버 개인정보보호 레시피

3-1. 경기도청 서버 스캔사례

3-2. 기관 및 기업 서버 스캔 활용 레시피



들어가며



파일서버나 DB서버는 장기간 기관 및 기업의 중요한 정보를 보관하고 활용하는 용도로 사용됩니다. 서버 내의 데이터가 잘 관리되어 운영된다면 이상적이겠지만, 현실적으로 방대한 양의 데이터가 관리되지 않은 채 방치되어있는 경우가 많습니다. 담당자가 바뀔 때 마다 새로 생기는 운영방침, 데이터 구분 방법도 한 몫을 합니다. 그렇게 수 년이 지나면 '구석기 화석이 나올 것만 같은(?)' 서버가 만들어집니다.

문제는 이러한 서버 안에 개인정보가 포함된 파일이나 데이터가 있을 확률이 매우 높다는 것입니다. 과거의 기관이나 기업은 무조건적으로 '고객정보를 많이 모으고 보는' 수집 방법을 활용했습니다. 그것이 소위 '잘하는 마케팅영업'이었습니다. 하지만 많은 개인정보보호법 시행 이후 많은 변화가 있었습니다. 현재 개인정보보호법 및 정부에서는 '개인정보 수집제한 및 암호화', '정보파기'와 같은 기술적/관리적 요구를 합니다.

그러다보니 보안 담당자는 골머리를 앓습니다. 대부분의 개인정보 유출사고는 DB서버에 유효기간이 지났는데도 방치되어오던 개인정보였습니다. 이미 모아버린 개인정보가 너무 많은데다가 어디에 있는 지도 알 수 없기 때문입니다. 내년 8월까지('16.08.06) 서버 어딘가에 방치되어있는 개인정보를 찾아서 파기해야 하는 이슈가 생긴 이 시점에 설록홈즈 보안 백서 시리즈, '서버 개인정보 진단 레시피'에서는 서버 개인정보보호가 필요한 이유부터 기술적 방안을 쉽게 설명하고자 합니다. 지금부터 차근차근 따라오시기 바랍니다.



1 서버 개인정보보호와 관련법

1-1. 개인정보보호법

개인정보보호법은 첫 시행 이후에 여러 번의 개정이 이루어지면서 더욱 강력한 기술적 보호조치 의무를 부과하고 있으며 처벌 범위도 넓어졌습니다. 과거에는 주민등록번호를 정보주체의 별도 동의를 받으면 수집할 수 있었지만 이제는 ‘법령상 근거’가 없다면 아예 모을 수가 없습니다. 이는 작년 8월(2014.08.07) 개인정보보호법 개정안 중 하나인 ‘주민번호 수집 법정주의’에 의한 것입니다.

‘주민번호 수집 법정주의’ (제 24 조의 2)

**주민번호 처리를 원칙적으로 금지하고, 예외적인 경우에만 허용
기 보유한 주민번호는 법 시행 후 2년 이내(‘16.8.6 까지) 파기**

〈주민번호 예외적 처리 허용 사유〉

1. 법령(법률·시행령·시행규칙)에서 구체적으로 주민번호 처리를 요구·허용한 경우
2. 정보주체 또는 제 3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우
3. 기타 주민번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

주민번호 수집 법정주의에서 눈여겨 봐야 할 것은, 바로 기 보유한 주민번호는 법 시행 이후 2년 이내(‘16.8.6 까지) 파기해야 한다는 점입니다. 법령 근거가 없다면 수집하지 말고 이미 보유했다면 파기하라는 조항입니다. 개인정보보호법에서 ‘파기’란 ‘복구 및 재생이 불가능한 방법’의 완전삭제를 의미합니다. 이 방법은 프로그래머가 아니라면 알고리즘을 써서 개인이 수동으로 삭제하기란 불가능하므로 보통 파기솔루션을 활용해 진행하게 됩니다.

만약 법령에 근거 없이 주민등록번호를 수집 및 이용하거나 제공할 경우 3천만원 이하의 과태료가 부과되며, 적법하게 수집했다라도 안전하게 관리 하지

않아 주민등록번호가 유출되면 최고 5원원의 과징금이 부과됩니다. 또한 2016년 8월 6일까지 이미 보유중인 법적 근거 없는 주민등록번호를 파기하지 않는다면 3천만원 이하의 과태료가 부과됩니다.

1-2. 정보통신망법 (정보통신망 이용 촉진 및 정보보호 등에 관한 법률)

정보통신망법은 정보통신서비스를 제공하는 사업자 대상의 특별법입니다. 적용대상은 정보통신망을 영리로 사용하는 273만개 사업자와 160만개 스마트폰 앱입니다. 인터넷을 통해 재화/서비스를 판매하는 경우 이에 해당합니다. 정보통신망법에서는 개인정보 미파기 시 유출되지 않아도 유출과 동일한 ‘형사처벌’을 진행하는 개인정보 미파기죄를 신설했습니다.(2014.05.28 개정, 2014.11. 29 시행)

제29조(개인정보의 파기)

- ① 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.

2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조)

기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자

제 29 조제 1 항을 위반하여 개인정보를 파기하지 아니한 자

제29조 개인정보의 파기의 경우 개인정보보호법에서 이야기하는 ‘복구 및 재생이 불가능한’ 방법의 파기방법을 그대로 가져왔습니다. 개인정보보호법과 다른 점이 있다면 유출이 되지 않아도, 파기 미 이행 시 2년 이하의 징역 또는 2천만원 이하의 벌금이라는 벌칙이 추가된 점입니다.

법령상 근거가 없는 주민번호 수집(주민번호수집금지 위반)의 경우 제76조 1항2호에 의해 3,000만원 이하의 과태료가 부과됩니다.

또한 제75조(양벌규정)에 따라 행위자를 벌하는 것 외에 법인에게도 벌금형을 부과하게 되는데, 행위자란 단순 유출행위를 한 직원만을 의미하는 것이 아닙니다. 특히 조치 미 이행의 경우 CEO가 행위자가 될 수 있습니다. 2014년 이후 CEO 책임에 초점을 두면서 CEO가 결재 하지 않은 책임 사항으로 조치 미 이행의 원인을 묻고 있습니다. 즉 행위자인 CEO에 대한 형사처벌과 법인에 대한 벌금형이 양벌규정으로 진행됩니다. (다만, 법인은 위반행위 방지를 위하여 상당한 주의와 감독을 한 경우에는 처벌하지 않습니다.)

2 서버 개인정보보호 이슈

관련 법령들의 대상은 개인정보 처리시스템 전체입니다. 개인정보 처리시스템이란 함은 DB서버, 파일서버, 웹서버, PC(데이터보관 시)와 같은 시스템을 의미합니다. 그렇다면 왜 서버 개인정보보호가 특히 이슈가 될까요?

2-1. 서버 개인정보보호

개인정보 유출 사고의 사례들을 살펴보면 웹서버나 DB서버에 존재하는 개인정보가 유출되는 경우가 대다수입니다. 개인정보 솔루션이나 암호화 솔루션을 도입하는 경우에도 적용 시 누락되는 서버들이 있어 방치되는 경우가 많기 때문입니다. 실제로 2014년 금융3사 개인정보 유출사건의 경우에도 개발 서버에 방치되어있던 개인정보를 협력직원이 USB로 무단 반출한 사례입니다. 관리자가 일일이 서버 개인정보 현황을 파악하기 힘든 것도 유출사건의 원인입니다. 주기적으로 서버를 관리하는 관리적, 기술적 보호조치를 진행하지 않기 때문입니다.

그리고 서버 또한 개인정보보호법에 따른 ‘개인정보 위험도 분석’이나 ‘개인정보 현황 분석’ 시 점검이 필요한 부분이며 영향평거나 개인정보 파일 일제 점검의 대상이 됩니다. 외부에 노출되어있는 WAS서버나 암호화 한 DB일지라도 메모리나 임시DB에 평문 상태로 방치되어있는 경우 해킹의 위험이 매우 큼니다. 어떻게 보면 서버는 개인정보보호 분야에서 가장 취약한 부분일 수도 있습니다.

2-2. 서버 개인정보보호 STEP

서버 개인정보보호 관련법을 정리해보면 ‘수집금지’와 ‘파기’ 두 가지 키워드를 파악 할 수 있습니다. 다만, 이미 수집한 개인정보가 대다수 이므로 파기 이전에 ‘진단(스캔)’을 통해 현황을 파악해야 하는 이슈가 존재합니다. ‘수집금지’, ‘진단’, ‘파기’ 세 가지 키워드를 통해 서버 개인정보보호 STEP을 알아보도록 하겠습니다.

〈서버 개인정보보호 STEP〉

1. **[진단]** 사실상 모아서는 안 되는 개인정보가 서버에 있는 지 진단(스캔)한다.
2. **[통계]** 현황을 파악한다. (통계, 대시보드 등을 통해 정리할 수 있다.)
3. **[암호화]** 보관해야 할 개인정보 경우 암호화를 진행한다. (DB암호화 등)

주민등록번호의 경우 법령 근거가 있어야 합니다.

주민등록번호의 경우 개인정보보호법 16년 1월 1일 ‘주민등록번호 암호화 의 무조항’ 시행에 의해 암호화하여 보관하여야 합니다.

4. **[파기]** 불필요 개인정보의 경우 복구 및 재생이 불가능한 방법으로 파기한다.

복구 및 재생이 불가능한 방식 중 컴트루테크놀로지는 미 국방성 인증을 받은 알고리즘을 활용하고 있습니다. 데이터를 7번 덮어쓰워 원본을 삭제하는 방식입니다. 이 방법으로는 복구가 불가능하여 파기 시 신중하게 진행해야 합니다.

2-3. 서버 개인정보 검출 관리 솔루션

개인정보보호법에 따른 서버 개인정보보호 STEP을 수행하기 위해서는 각종 서버 내 개인정보를 검출하고 관리하는 솔루션이 필요합니다. 관리자가 일일이 서버 속 데이터를 확인하여 개인정보를 찾아내기란 백사장에서 바늘 찾기과 같기 때문입니다.

〈설치방식에 따른 솔루션 구분〉

서버 개인정보보호 솔루션은 크게 두 가지 방식이 있습니다. 어플라이언스방식과 에이전트방식입니다. 어플라이언스 방식은 서버 앞단에 H/W와 S/W 일체형 어플라이언스를 연결하여 해당 장비가 스캔을 수행하는 방식입니다. 에이전트 방식은 각 서버에 에이전트(S/W)를 설치하여 각 에이전트가 스캔을 수행하고, 관리서버가 에이전트를 관리하는 방식입니다.

방식	어플라이언스 방식	에이전트 방식
특징	초기설치가 쉽다. (서버 앞단에 연결) 새로운 서버가 생겨도 연결 후 진단이 가능하다. (유지관리편의)	해당 서버 내에서 검출하므로 보안성이 높다. 네트워크 부하가 없다.

〈표1. 서버 개인정보 검출 관리 솔루션 지원 방식〉

어플라이언스 방식은 초기 설치가 매우 쉽고, 여러대의 서버를 하나의 장비에서 관리 할 수 있으므로 효율적입니다. 향후 새로운 서버가 도입되어도 연결 후 진단 관리를 하면 되므로 유지 관리의 편의성이 있다는 장점도 있습니다.

에이전트 방식은 해당 서버 내에서 에이전트가 개인정보를 검출하므로 보안성이 높고 네트워크 부하가 없다는 장점이 있습니다.

컴트루테크놀로지는 서버 개인정보보호 솔루션인 설록홈즈 PrivacyCenter-S 서버스캔에서 **국내 유일하게 어플라이언스 방식과 에이전트 방식 두 가지를 모두 제공하고 있습니다.**



〈그림1. 어플라이언스 및 에이전트 방식〉

〈설록홈즈 PrivacyCenter-S 서버스캔 소개〉



〈그림1. 설록홈즈 PrivacyCenter-S 서버스캔 로고〉



〈그림2. 등록 및 인증 현황〉

설록홈즈 PrivacyCenter-S 서버스캔의 경우 9년 연속 시장점유율 1위의 홈페이지 개인정보보호 솔루션 ‘설록홈즈 PrivacyCenter’의 자매 제품입니다. 서버스캔의 경우 파일서버와 DB서버에 있는 개인정보를 스캔하여 검출하고 유용한 관리를 도와주는 솔루션입니다.



〈그림3. 설록홈즈 PrivacyCenter-S 서버스캔〉

파일서버 및 웹서버, DB서버에서 개인정보를 검출하고 이를 관리 할 수 있도록 다양한 기능을 제공하고 있습니다. 서버 개인정보보호 솔루션을 고려할

때 알아두어야 할 사항에는 무엇이 있을까요?

〈‘필터링’ 능력〉

필터링 능력은 ‘어디에서’ ‘얼마나 잘’ 개인정보를 검출할 수 있는지에 대한 부분입니다. ‘어디에서’의 경우, 예를 들어 지원 DB서버 종류(Oracle, My SQL, MS SQL 등)를 파악하여 우리 기관 및 기업에 존재하는 서버를 모두 스캔 할 수 있는 지 알아보아야 합니다. ‘얼마나 잘’의 경우 필터링 기술력에 달려있습니다. ‘필터링 기술’의 질은 개인정보 패턴 지원 종류와 정확성등에 따라 좌우 됩니다. 이 기술에 따라 서버 속 개인정보를 찾아내게 되므로 가장 중요한 고려사항이라 볼 수 있습니다.

우수한 필터링 능력으로 공공기관 프로젝트 참여 사례

- 2008년 공공기관 홈페이지 개인정보 노출 방지를 위한 상시 모니터링 및 컨설팅 사업 참여
- 공공기관의 개인정보 검출 능력을 인정 받고 선발되어 프로젝트 수행
- 공공기관의 다양한 개인정보 패턴 검출 능력 보유

설록홈즈 PrivacyCenter 레퍼런스 (약 500여개, 시장점유율 1위)



〈보안성 고려〉

DB서버에서 DB데이터를 통째로 복사하여 사본 테이블을 만든 뒤 사본 테이블에서 검출을 진행하는 기존의 방식은 보안상 위험이 될 수 있습니다. 그렇기 때문에 DB서버의 문자열만으로 검출을 하고 바로 삭제를 진행하며, 사본이나 별도 백업된 테이블이 남지 않도록 보안성을 고려하는 방식을 활용해야 합니다.

<후처리>

검출만 진행하고 끝난다면 관리자의 고민은 아직 끝난 것이 아닙니다. 후처리를 통해 보관하지 않아야 할 개인정보를 치환(마스킹)이나 완전삭제를 해야 합니다. 후처리의 경우 다시 복구가 불가능하므로 신중히 진행해야 한 다는 것을 기억하세요.



더 알아보기

서버뿐만 아니라 PC에 있는 개인정보도 관리해야 하나요?

서버 외에도 PC에 있는 주민등록번호(개인정보) 또한 법령상 근거가 없다면 완전삭제해야 합니다. 행자부나 방통위 감사 시 PC에 있는 개인정보 여부는 항상 파악하는 항목이기도 합니다. PC에 엑셀과 같은 데이터베이스형태로 개인정보가 있다면 PC도 개인정보처리시스템으로 보기 때문입니다.

서버와 마찬가지로 사람이 수동으로 파일을 찾아 암호화 하거나 삭제하기는 힘이 들므로 별도 솔루션을 활용합니다. PC에 있는 개인정보를 진단하고 암호화 및 완전삭제를 진행하며, 에이전트를 PC에 설치하는 방식으로 진행됩니다.

[> \[클릭\] 설록홈즈 PC스캔 알아보기](#)

3 서버 개인정보보호 레시피

3-1. 경기도청 서버 스캔사례

■ 경기도청 서버 개인정보보호 사례



경기도청은 빅데이터 관련 사업을 진행하면서 빅데이터 수집 서버에 있을 수 있는 개인정보 노출을 방지하고자 서버 스캔을 진행하고 있습니다. 경기도청 행정망 및 외부망의 데이터가 1차로 집합되는 저장소에 대해 서버 스캔을 진행하며 개인정보 여부를 관리자에게 알려줍니다.

1차 집합 저장소에서 외부로 공개되기 전에도 한 번 더 검사를 진행하여 외부망으로의 개인정보 공개를 통제할 수 있습니다. 빅데이터 활용 시 가장 문제되는 Privacy침해 문제를 해결 할 수 있는 서버 스캔의 사례입니다.

3-2. 기관 및 기업 서버 스캔 활용 레시피

- 재료 :  설록홈즈 PrivacyCenter-S 서버스캔 , 방치된 서버
- 조리방법 :

1. 서버 현황 파악



기관 및 기업에서 개인정보가 있을 것으로 파악되는 DB서버 및 파일서버 현황을 파악합니다. 각 서버의 용도와 운영여부, 서버 접속정보를 파악하여 기록합니다.

2. 검출정책 세우기



어떤 서버에서 개인정보를 검출해야 하는지 정책을 세웁니다. 미운영 서버의 경우 1회 진단을 통해 개인정보 유무를 파악하고 관리 할 수 있으며, 운영 서버의 경우 예약 진단을 통해 주 단위, 월 단위로 지속적인 개인정보 유무를 파악할 수 있을 것입니다.

각 서버 접속정보를 기입한 뒤에는 어떠한 개인정보를 검출 할 지 선택합니다. 주민등록번호, 외국인번호, 여권번호, 운전면허번호 등 고유식별정보의 경우 선택을 해 주는 것이 좋습니다. 설록홈즈 PrivacyCenter-S 서버스캔은 국내에서 가장 많은 개인정보 패턴을 제공하고 있습니다.

3. 검출하기



검출을 진행하게 되면 총 파일 수, 스캔 한 파일 수, 검출된 파일 수 등 각종 통계 값을 파악할 수 있습니다. 각 개인정보 패턴 별로 얼마나 많은 개인정보가 검출 되었는지도 파악 할 수 있습니다. DB 서버의 경우 어떤 컬럼의 어떤 레코드에 개인정보가 있는지도 나오게 됩니다. 해당 자료는 엑셀 다운로드로 보고서로 활용 할 수 있으며 개인정보현황을 파악하는 자료로 활용할 수 있습니다.

4. 치환 또는 파기를 통해 관리하기



검출 후에는 해당 개인정보를 치환(마스킹)하거나 완전삭제를 통해 관리 할 수 있습니다. 법에서 요구하는 것은 법령상 근거가 없는 개인정보(주민번호)를 보관하지 않고 법 시행 이후 2년 이내인 2016년 8월 6일까지 파기하는 것이므로 매우 중요한 단계라 볼 수 있습니다. 치환은 *표 표시등으로 주민등록번호 뒷자리를 없애 고유식별정보인 '주민등록번호'를 '생년월일'로 변경시키는 방법을 말하며, 완전 삭제는 불필요한 개인정보를 아예 서버에서 삭제하는 방법을 말합니다. <마침>

〈백서보고 궁금하다면〉
서버스캔
무료 체험신청 (CLICK 하세요)

