# DW(DataWarehouse) 고객식별자정보 유출 방지를 위한 시스템 구현 사례 연구

유재용*
*고려대학교 컴퓨터정보통신대학원 디지털정보미디어공학과
e-mail : jaeyong07@korea.ac.kr

# A Study on DataWarehouse for Client's Distinguish Information Protection System

Jae-Yong Yu*
*Graduate School of Computer and Information and Technology, Korea University

**요 약**

기업 내부적으로 고객의 정보를 다루는 DataWarehouse 시스템에 대한 활용도가 증대되고 있다. 특히 고객 식별자 정보(주민번호, 고객성명, 전화번호, E-mail, 주소)에 대한 접근을 통해 데이터를 추출하여 분석하고 이를 마케팅이나 고객 Segment 를 위해 활용이 증대되고 있다. 따라서 민감한 고객의 고객의 정보를 전사적인 차원에서 체계적인 관리를 위한 시스템이 필요하다. 본 논문에서는 DW 고객 식별자 정보 이용절차를 개선하여 대량정보 유출 및 불법 이용을 사전에 예방하고 사후 보안 체계를 강화하는 시스템을 구현 모델을 설명하며, 그 결과로 사용자, 관리자, 감사자까지의 각 단계별 검증 프로세스를 통한 고객 식별자 정보 관리의 극대화 방향을 제시한다.

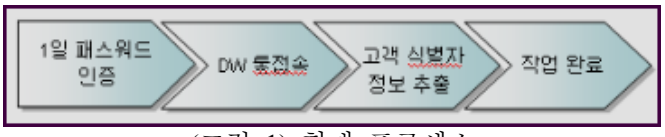
## 1. 서론

최근 개인정보의 유출 및 변조 사고로 인하여 기업의 이미지 손실에 큰 영향을 주고 있으며 사고의 약 80%는 내부 사용자와 연관이 있다. 현재 전사 고객 정보를 보유하고 있는 DW(DataWarehouse)내에 허가된 권한을 가진 사용자는 고객 식별자 정보[1]를 쉽게 접근하여 이용할 수 있다. 시스템 내의 1 일 패스워드 인증 후 무제한 접근을 통해 데이터의 무분별한 추출이 발생되게 된다. 또한 추출된 데이터의 이력 추적이 복잡하고 수작업 방식으로 이용 현황을 분석하고 있다. 이러한 정보 관리의 활용에 관한 접근통제 및 이력관리의 시스템화가 대두되었다.

본 논문은 다음과 같이 구성된다. 제 2 장에는 운영중인 프로세스를 중심으로 DW 의 사용자 승인에서 데이터 추출 및 활용까지의 일련의 과정과 문제점을 제시하고 3 장에서는 고객식별정보 유출 방지를 위한 시스템 구현 및 구축 사례를 중심으로 설명하며 4 장에서는 결론 및 향후 연구를 기술하고자 한다.

## 2. DataWarehouse 운영 프로세스 및 문제점

일반 사용자가 DW 의 권한을 취득하기 위해서는 몇 가지 승인 절차가 필요하다. 우선 사용자가 부서내의 최종관리자 승인을 취득한 후 DW 관리부서에 사용자




(그림 1) 현재 프로세스

의 활용 목적과 사용자 확인 후 권한을 부여한다. 그리고 사용자는 일일 1 회의 패스워드 부여를 위한 별도의 신청과 담당부서의 승인을 취득하여 DW 에 접속하게 된다. 이후 사용자는 자신이 원하는 쿼리를 쿼리 툴을 통하여 데이터 추출을 의도적 또는 비의도적인 목적을 가지고 고객식별정보를 활용을 한다. 이런 측면에서 접근 통제의 체계적인 관리가 요구되어졌으며,이후 데이터에 대한 감사추적성(Accountability)에 대한 문제가 발생된다.

매일매일 발생되는 모든 쿼리에 대한 분석 및 관리를 실시간 이루어내기란 어려운 일이다. 또한 모든 사용자들이 다양한 형태의 사용자에게 한번 권한을 부여받은 후 지속적인 데이터 추출은 하루 수천만, 수억건의 데이터 처리가 발생됨으로 DW 시스템에 과부하를 일으키게 된다.

## 3. 고객식별정보 유출 방지를 위한 시스템 구축사례

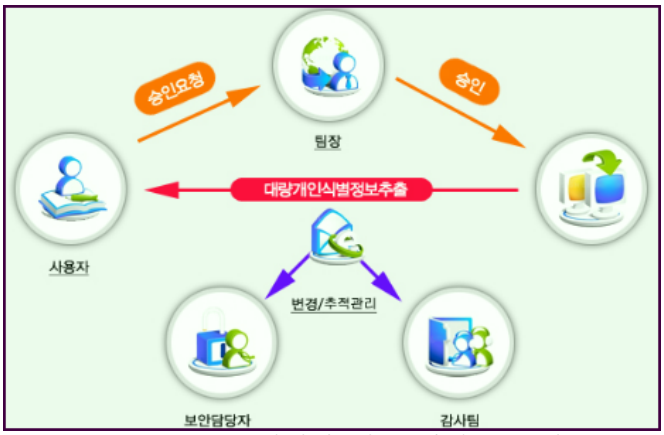
### 3.1 시스템 설계 및 구현

고객 식별자 정보 시스템의 운영체계는 유닉스 바탕으로 .NET FrameWork 와 Sybase ASE 를 연동한 C/S 화면으로 구성되었다. 사용자는 client 설치를 통한

[1] 고객 식별자 정보는 주민번호, 고객성명, 전화번호, E-mail, 주소의 5 개 항목을 포괄하는 의미.

사용자 인증 방식을 통한 로그인이 가능토록 하였다. 서버상에서 처리되는 쉘 스크립트로 구현된 데몬 프로세스를 통한 실시간 사용자의 데이터 추출이 가능토록 구현하였다. 고객 정보를 추출하는 사용자는 고객 식별자 정보 시스템의 로그인을 통한 후 데이터의 접근이 가능토록 되어 있다.

또한 사용자, 관리자(팀장), 보안담당자, 감사자의 업무 권한을 도입하여 관리기능을 강화하였다.




(그림 2) 고객 식별자 정보 처리 프로세스

♦ 현업 사용자
- 데이터 추출을 위한 1 건의 SQL 작성 후 부서내 관리자에게 승인요청과 동시에 관리자에게 자동 메일 발송되며, 인가된 목적 외에는 사용이 제한된다.

♦ 관리자(팀장)
- 사용자가 요청한 정보의 활용 목적, 이용건수, 데이터 보존기간 등의 정보를 확인할 수 있으며, 승인 완료시에는 사용자에게 자동 메일이 발송되며, 데이터 추출 작업이 진행된다.

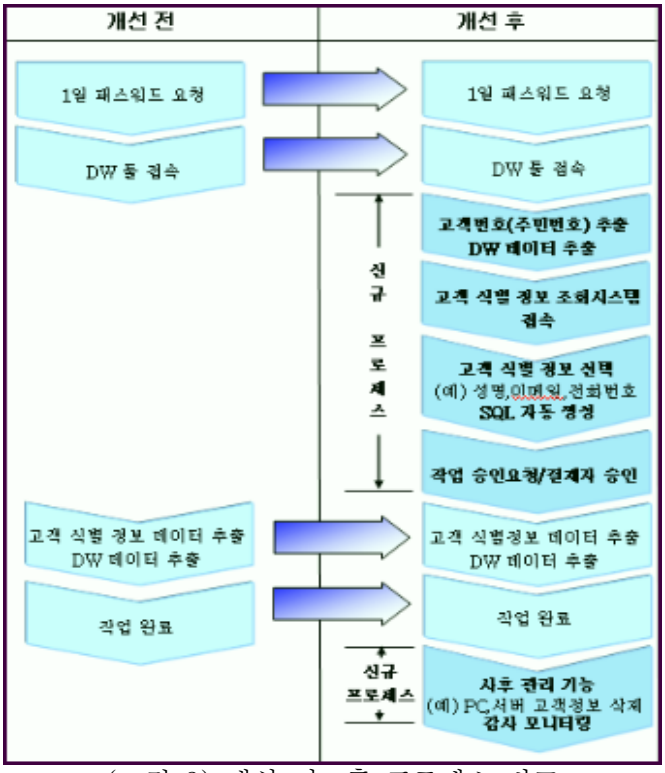
♦ 정보보호담당자
- 부서내 고객 식별자 정보에 대한 활용에 대한 데이터 파일의 삭제 및 감시를 담당하며, 데이터 삭제 후 사용자, 관리자에게 메일로 데이터 삭제가 통보된다.

♦ 감사팀(감사자)
- 전사의 고객 식별자 정보의 작업 수행에 관련된 업무를 모니터링 하며, 일별/월별 및 사용자별/시간대별 사용내역 확인을 통한 실시간 감사가 가능하다.

### 3.2 효율적 관리 프로세스 기능

사용자의 1 일 패스워드 발급 후 의도적이거나 비의도적인 목적으로 쿼리를 통한 데이터 추출이 가능했지만 이용 건별 관리자의 결제 후 데이터 추출이 가능토록 변경하여 Ad-hoc 쿼리의 생성을 줄였고 시스템의 부하도 예방할 수 있다. 데이터 사용의 이력의 추적의 어려움을 극복하기 위하여 데이터의 조회->추출->활용->폐기의 단계별 정보 관리를 수행하였다. 생성된 데이터는 툴 기동시 자동삭제 기능을 추가하여 이용기간 경과후 자동삭제 하도록 구현 하였으며, 부서내 정보보호 담당자를 통하여 2 차적으로 삭제 및 확인이 가능토록 백업 장치를 마련하였다.

감사자 및 관리자는 전사 또는 부서내의 이용현황에 대한 기간별 분석이 가능하도록 하여 수작업으로 관리되어 온 이용현황 시스템을 자동화하여 필요시마다 정보 통계에 대한 활용을 가능토록 하였다.




(그림 3) 개선 전 · 후 프로세스 비교

## 4. 결론

최근 몇 년동안 기업 고객정보의 유출은 지속 가능한 경영에 커다란 영향을 주었다. 고객 식별자 정보 시스템을 통한 DB 접근제어, 고객 식별자 정보의 체계적 관리 그리고 사후관리 및 모니터링을 기능을 통한 관리를 수행하고 있다. 본 논문에서 제시한 모델을 통하여 기존의 고객 식별자 정보의 활용의 문제점을 해결하여 사용자별 업무 처리 권한과 사후관리 모니터링 기능을 추가하여 사용 및 관리의 편리성을 도모하였다. 향후 연구로는 추출된 파일의 변경이 불가능하도록 하여 데이터의 사후관리 측면에 대한 보안을 더욱 강화할 수 있는 방법을 제시하겠다.

## 참고문헌

[1] 이윤호, “기업의 정보 유출방지를 위한 개인정보 전송시스템에 대한 연구”, 동국대 국제정보대학원 (2009.02)

[2] 문진규,”내부정보 유출 방지를 위한 정보보호 기술구조 설계 및 구현에 관한 연구”, 정보처리학회 춘계학술발표대회 논문집(2007.05)

[3] 김종원, 최종욱,“기업 정보 유출 방지를 위한 기술”, 정보처리학회(2003.03)

[4] 김정상,“개인정보 침해사례를 통한 데이터베이스 보안에 관한 연구”, 건국대 정보통신대학원(2007.08)