情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

SAP DB 암호화에 대한 고찰

황 치 하*, 박 준 성**, 최 재 우***, 김 학 범****

요 약

개인정보보호법에 따라 기업에서는 현재 사용하고 있는 ERP시스템의 개인정보 암호화를 수행해야만 한다. 특히 국내 주요 기업에서 사용되고 있는 SAP 시스템의 DB암호화는 SAP솔루션의 특성을 고려하여 일반 DB암호화와는 다르게 접근해야 한다. 이 논문에서는 SAP DB의 특성과 대표적인 SAP DB암호화 방법에 대해 고찰해보고자 한다.

Ⅰ. 서 론

1. DB암호화에 대한 필요성

개인정보의 유출과 이를 이용한 범죄가 증가함에 따라 2011년 3월 개인정보보호법이 제정되었다. 이에 행안부에서는 [개인정보의 안전성 확보조치 기준 및 해설서]를 통해 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적·관리적 보호조치 등의 세부기준을 제시하였다.

기준에 따르면 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보이며, 개인정보처리자는 개인정보를 정보통신망을 통하여 송·수신하거나 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여야 한다. “안전한 암호 알고리즘”이란 미국 NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 및 국내외 암호 연구기관에서 권고하는 알고리즘을 의미한다[1].

2011년 9월부터 개인정보보호법이 시행됨에 따라 공공기관 뿐만 아니라 많은 기업에서 개인정보보호 암호화를 수행하고 있다. 특히 기업의 경우 비즈니스와 서비스를 위해 많은 고객의 개인정보를 수집, 저장한다. 최근 급증하는 보안위험과 돈을 목적으로 하는 해킹이 증감함에 따라 개인정보보호를 위한 투자를 더 이상 늦출 수 없게 되었다. 하지만 개인정보 암호화에 따른 성능문제나 어플리케이션을 수정해야하는 문제 등 DB암호화 기술에 대한 부작용이 존재하기 때문에 암호화에 대한 이해와 고찰이 필요하다.

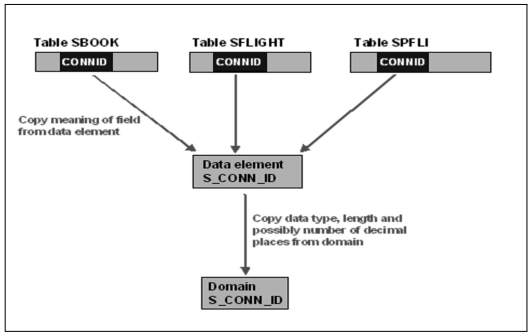
본문에서는 국내 ERP시스템에 많이 사용하고 있는 SAP 시스템에 대한 특성을 파악하여 SAP DB암호화에 대한 이해와 방안에 대해 고찰하고자 한다.

Ⅱ. SAP DB의 특징

일반 DB의 경우 암호화를 적용하려면 개인정보의 길이가 늘어나거나 타입이 변경되고 원시테이블의 구조의 변경이 필요하다. 이러한 변경은 응용시스템 수정이나 심각한 DB성능 저하의 문제를 발생시킬 수 있다. SAP DB의 경우 일반 DB암호화 방식으로는 구현이 불가하다. SAP DB에서 데이터 구조의 변경에 여러 가지 제약을 가지고 있다. 그래서 일반 DB암호화와는 다른 접근방식이 필요하다. 지금부터 SAP 시스템과 DB의 특성에 대해 살펴보고자 한다.

첫째 SAP Table은 잘 정의된 Data element를 이용하여 데이터 유형의 표준화 및 가독성을 높이는 구조를 가지고 있다.

* 동국대학교 국제정보보호대학원 정보보호학과 석사과정 (lovesong2143@naver.com)
** 동국대학교 국제정보보호대학원 정보보호학과 석사과정 (juns1982@gmail.com)
*** 동국대학교 국제정보보호대학원 정보보호학과 석사과정 (vjwchoi@gmail.com)
**** ㈜지엔에스인증원/동국대학교 국제정보대학원 정보보호학과 (khb0305@gns-iso.co.kr)



〔그림 1〕 SAP Data element[2]

SAP솔루션에서 Domain은 Field의 데이터 유형과 길이 등 기술적인 속성을 정의한다. Data element는 Table Field의 모든 정보를 가지고 있는 Object이다. Data element는 Domain의 기술적인 속성을 참조하여 Field의 속성을 정의한다. 물론 Field를 정의할 때 반드시 Data element를 써야만 하는 것은 아니지만 프로그램 개발의 품질과 생산성을 위해 Data element를 이용하여 Field를 정의한다[3].

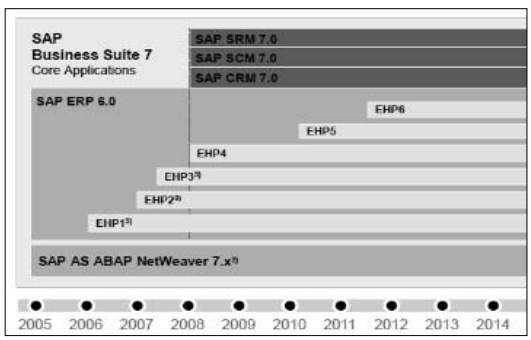
SAP DB암호화 적용 시 일반 DB암호화 방식을 적용하게 되면 데이터의 속성이 변경되고 Table 구조 변경이 필요하다. 결론적으로, Domain의 속성이 변경되고 여러 Table이 영향을 받게 된다. SAP DB암호화 적용 시 이와 같은 특성을 고려하여 개인정보를 저장한 Field의 Data element가 여러 테이블에 영향을 주는 경우 동일한 데이터 타입을 갖는 Domain을 생성하여 암호화를 적용하는 방법을 고려해야 한다.

둘째로 SAP솔루션은 지속적으로 변경과 업데이트가 적용된다. 이러한 기능과 프로세스의 변경은 데이터를 저장하는 SAP DB의 구조에도 영향을 끼친다. SAP솔루션의 로드맵을 보면 매년 새로운 기능이 제공되는 것을 볼 수 있다. 시장의 변화와 요구사항에 따라 선전업무 Process와 새로운 기능 추가가 빠르게 제공된다.

SAP솔루션은 표준기능에 영향을 미치지 않는 범위에서 추가 기능을 개발하는 것을 허용한다. 표준으로 제공하는 기능이나 프로세스가 회사의 환경에 맞지 않는 경우 일부 기능을 개발하고 추가할 수 있다. 이것을 CBO(Customer Bolt-On)라고 한다. 하지만 SAP 표준기능을 직접 변경하는 작업, 예를 들어 표준 Table의 Field를 변경하거나 프로그램 코드를 변경하는 것은 권장하지 않는다. 왜냐하면 SAP 기술구조에 대한 전체적인 이해 없이 표준 Table이나 프로그램을 수정할 경우 예기치 못한 문제가 발생할 수 있기 때문이다. 또한 버전 업그레이드 시 반영이 되지 않기 때문에 계속적인 유지보수의 부담을 회사가 감수해야 한다. 따라서 SAP 표준기능에 대한 이해를 바탕으로 SAP DB암호화에 대해 접근해야 한다.

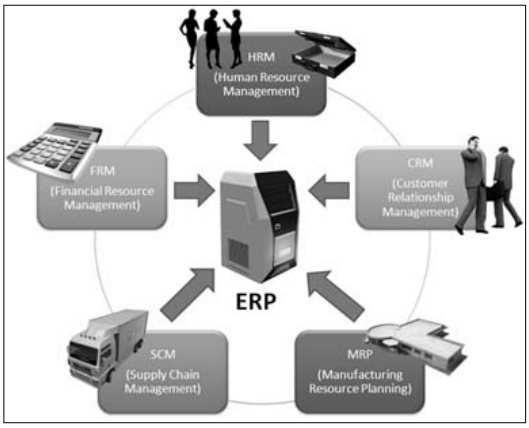
셋째로 SAP솔루션은 기업 활동 수행을 위한 여러 시스템 즉, 생산, 판매, 인사, 회계, 자금, 원가 등 경영자원을 하나의 체계로 구축한 ERP(통합정보시스템)시스템이다.

전사의 자원들을 SAP으로 통합하기 때문에 시스템 간 많은 인터페이스가 발생한다. 또한 실시간으로 데이터를 처리하기 때문에 시스템들이 유기적으로 연결되어 있어서 어느 한 시스템에서 입력을 하면 연관된 시스템들로 자동으로 정보가 전달된다. 글로벌한 기업의 경우 24시간 365일 가동되기 때문에 암호화 적용 시 업무 중



〔그림 2〕 SAP Business Suite 7 Innovation Road Map[4]

* EHP(Enhancement package) : 새로운 기능 또는 개선된 비즈니스 기능을 포함한 패키지로 선택적인 적용이 가능함



〔그림 3〕 ERP시스템[5]

단이나 장애에 대응할 수 있는 준비와 연관된 시스템의 영향도 분석을 철저히 수행해야 한다.

Ⅲ. 토큰 암호화

일반 DB에서는 Plug-in방식이나 API방식을 이용하여 DB암호화를 적용함에 따라 테이블 필드의 구조변경으로 인해 성능저하의 문제가 발생한다. 하지만 토큰(Token)을 이용하는 방법은 테이블 필드의 구조변경이 없고 기존 DB인덱스 성능을 유지할 수 있다. SAP솔루션의 특성을 고려하여 SAP DB암호화에서는 토큰을 이용한 암호화 방식을 많이 사용한다. 토큰이란 암호화하려는 개인정보를 대체하는 임의의 값이다. 토큰은 데이터의 속성을 유지하고, 랜덤하게 생성되며 중복없이 원본 데이터와 매핑되는 특성을 가진다.

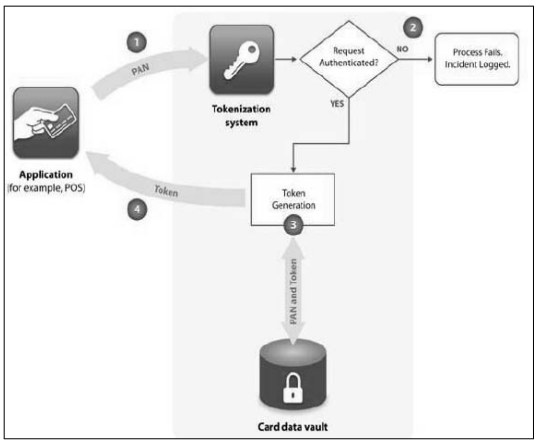
토큰을 이용한 암호화 방식은 크게 랜덤토큰 방식과 FPE(Format Preserving Encryption)토큰 방식으로 구분할 수 있다.

3.1. 랜덤토큰 암호화 과정

아래 그림을 통해 랜덤토큰 암호화 과정을 살펴보자.

Step 1. 응용시스템을 통해 수집된 고객정보나 개인정보는 토큰서버로 전달한다. 토큰서버에 접속하기 위해서는 반드시 인증절차를 거쳐야 한다.

Step 2. 토큰서버는 개인정보를 전달한 응용시스템이 적절한 인증을 거쳤는지 검증을 수행한다. 만약 검증결과 인증에 실패하면 토큰화 프로세스는 종료가 되고 모니터링을 위해 실패로그를 저장한다. 인증에 성공하면 Step 3을 수행한다.



〔그림 4〕 토큰 암호화 과정[6]

Step 3. 토큰서버는 인증된 응용시스템이 전달한 개인정보와 동일한 데이터가 있는지 검색을 한다. 신규 데이터인 경우 토큰을 생성하고 개인정보는 암호화하여 토큰과 함께 DB에 저장한다.

Step 4. 토큰서버는 Application에게 토큰값을 전송하고 Application은 토큰화된 개인정보를 Application DB에 저장하거나 사용한다.

3.2. 랜덤토큰 암호화 보안 고려사항

랜덤토큰 방식을 사용할 때 몇 가지 고려해야할 보안요소가 있다.

첫째로 네트워크에 대한 보안이다. Application과 토큰서버가 통신하는 구간은 외부 인터넷 구간이나 신뢰할 수 없는 네트워크와 독립적으로 구성되어야 한다. 네트워크를 통해 평문으로 개인정보가 송수신되기 때문에 안전한 네트워크 구성이 필요하다.

둘째로 토큰서버는 접속요청에 대해 강력한 접근통제 기능을 제공해야 한다. 접근하는 application, 사용자, 프로세스, 시스템에 대해 적절한 수준의 인증기능을 제공해야 한다. 암복호화를 요청하는 주체를 정확히 식별하고 암복호화에 대한 권한을 확인하여 데이터에 대한 접근을 통제해야 한다.

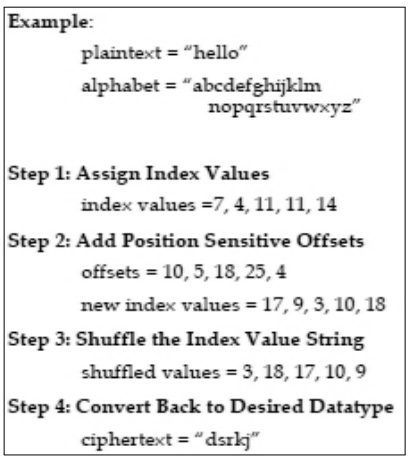
셋째로 모니터링 기능이 있어야 한다. 토큰서버에서 접근하는 모든 주체와 행위에 대해 로깅을 해야 한다. 부적절한 방법으로 접근하거나 의심스러운 사용자에 대해서도 탐지와 알람을 줄 수 있어야한다.

넷째 랜덤토큰을 이용하여 암호화하는 솔루션은 토큰과 실제 데이터를 구별할 수 있는 방법을 제공해야 한다. 생성된 토큰이 실제 데이터와 유사한 형태로 생성되어 구별이 어려운 경우 개인정보가 암호화되었는지 판단하기 어렵다. 암호화되지 않은 개인정보가 없는지, 암호화 실패한 이력은 없는지 검증할 수 있는 방안을 제공해야 한다.

마지막으로 토큰서버는 안전한 보안기능을 제공해야 한다. 모든 개인정보를 토큰서버 내에 저장하고 있기 때문에 보안위협으로부터 개인정보를 보호할 수 있는 강력한 통제기능이 필요하다[6].

3.3. FPE 토큰 방식 과정

토큰을 이용한 또 다른 방식인 FPE 방식은 1997년 Brigthwell에 의해 소개되었다. FPE는 데이터의 포맷을 변경하지 않는 암호화 방법으로 개인정보를 암호문으로 변환할 때 FPE(Format Preserving Encryption) 알고리즘으로 평문과 길이와 형태가 동일한 형태로 암호문을 만들어 대체하는 암호화 기법이다. FPE 의 기본 프로세스는 다음과 같다.



〔그림 5〕 FPE 기본 프로세스 예제[7]

Step 1. 처음 단계는 암호화될 텍스트의 각 스트링을 Index로 만든다. 이 때 생성되어지는 Index값은 제로(0)와 알파벳 문자의 총 수에서 1을 뺀 숫자 사이의 값이다. 텍스트 문자가 유효하지 않은 알파벳에 있는 경우, 아웃풋으로 카피되어 암호화된 스트링에서 삭제된다.

Step 2. 알파벳 인덱스 값을 할당한 뒤, 각각에 여러 정수 오프셋을 추가한다. 유효한 문자들(예: 알파벳에 포함된 문자들)만을 생성하기 위해 modular addition을 사용했다. 여기서 modular addition은 두 개의 숫자를 더한 다음 일정 "계수" 값을 나눈 나머지를 결정하는 것이다. 위의 예에서 알파벳 크기는 26이므로, 예를 들어 18 + 11 (mod 26) =3이다. 실제 오프셋 값은 데이터를 암호화하는데 사용하는 키의 값에 근거하여 생성된다. 이 단계는 일련의 길고 동일한 문자(문자 필드 끝에 20개 공백과 같은)가 동일하게 암호화 되는 것을 방지하기 위함이다.

Step 3. 오프셋을 더하거나 추가한 후, 전체 스트링을 셔플한다. 셔플링 방법은 인덱스 값의 치환불변 속성(모든 값의 총합 또는 모든 값을 제외한 값 등)에 따라 달라진다. 이 셔플링 단계는 공통 접두사 또는 접미사가 있는 텍스트가 공통 접두사 또는 접미사가 있는 암호텍스트를 생성할 수 없도록 한다. 특정한 데이터 특정적 상황에 대처하기 위해 상기 알고리즘에 두 가지 강화/보완 방법을 사용할 수 있다.

첫째, 인접 문자가 있는 두 개의 단일 문자 스트링의 인코딩된 값이 순차적이 되지 않게 하려면 (예, "a"가 "x"로 암호화 될 때마다 "b"가 "y"로 암호화되는 것은 원치 않을 때), 알파벳 자체를 암호화키의 portion에 따라 셔플할 수 있다.

둘째, 암호화된 문자 치환에 근거한 추측을 방지하기 위하여, 데이터를 왼쪽에서 오른쪽으로, 오른쪽에서 왼쪽으로 "ripple"할 수 있다. 이는 키를 "starter-digit"에 해싱하고 인접값을 쌍으로 추가하여 이루어진다. 예를 들어 인덱스 값 스트링 "1, 2, 3"은 다음과 같이 "23, 5, 40"으로 ripple 될 수 있다(55문자 알파벳이라 가정했을 때)[7].

3.4. FPE 토큰 방식 특징

FPE토큰 방식의 특징은 의미없는 토큰을 생성하는 것이 아니라 실제 데이터를 동일한 타입의 암호화된 토큰으로 만드는 방식이다. FPE토큰 방식에서 생성하는 토큰은 실제 데이터가 암호화된 값이기 때문에 암호화 알고리즘이 중요하다. FPE 알고리즘은 현재 미국국립표준기술연구소(NIST)에서는 FPE 알고리즘에 대한 연구가 진행되고 있다.

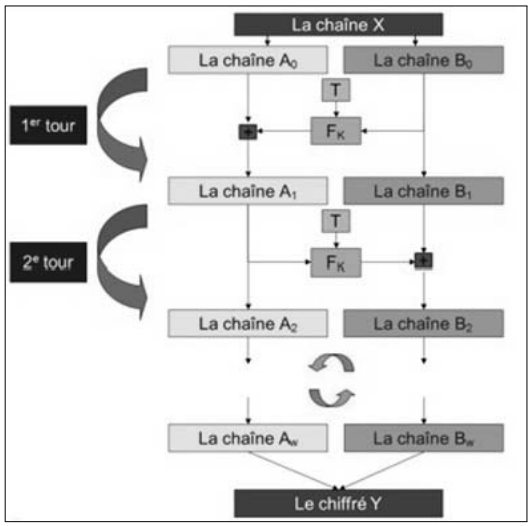
3.5. FPE 알고리즘

대표적인 FPE 알고리즘 3가지에 대해 살펴보자.

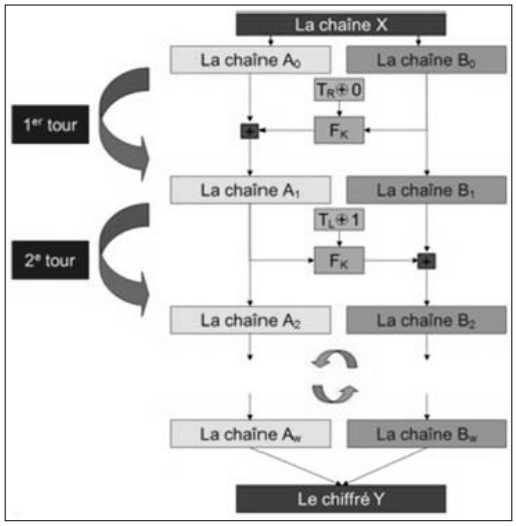
FFX(Format-preserving Feistel-based Encryption) 모드는 Key Fk와 Tweak T에 따라 유연성을 제공한다. FFX는 사용자가 정의한 Key에 따라 lifetime이 결정되고, round 수나 불규칙한 split, round 함수 등의 파라미터에 따라 커스터마이징이 가능하다. 암복호화 기능인 FFX.Encrypt 와 FFX.Decrypt 는 동일한 파라미터를 가진다[10].

〔표 1〕 FPE 알고리즘 비교[9]

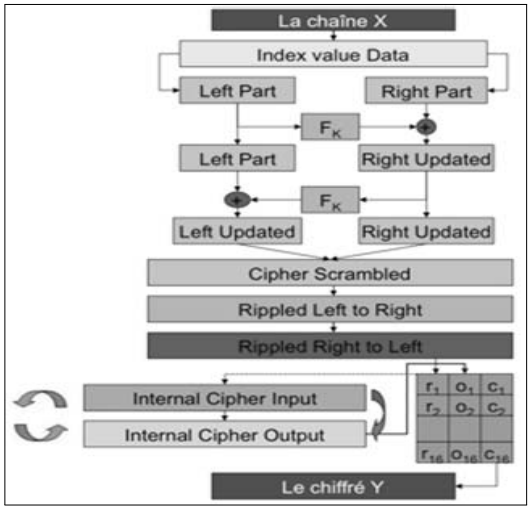
특징	FFX	BPS	FCEM
Feistel based	Yes	Yes	No
#Round	12	8	2
Cipher function	AES	AES/TDES/ SHA	AES
#Function is used	12	8	8
Reversibility	Yes	Yes	Yes
Tweak	Yes	Yes	No



〔그림 6〕 FFX 모드[9]



〔그림 7〕 BPS 모드[9]



〔그림 8〕 FECM 모드[9]

BPS(Format Preserving Encryption Proposal) 는 내부 고정길이 블럭 암호(TDES, AES, SHA-2와 같은 내부 함수)와 긴 문자열을 처리하기 위한 오퍼레이션 모드 2개의 컴포넌트로 구성된다 . BPS는 Cipher-Block Chaining mode(CBC mode)와 유사한 기능을 제공하며 효율적이다.[11].

FCE(Format Controlling Encrption)모드는 DTP (Datatype-Preserving Encryption)에 대한 확장이다. FCEM는 DTP에서 제한되었던 키 회전과 무결성 기능을 지원한다. 암호화된 문자 치환에 근거한 추측을 방지하기 위하여, 데이터를 왼쪽에서 오른쪽으로, 오른쪽에서 왼쪽으로 “ripple”하는 기능을 제공한다[12].

FPE 알고리즘은 암호화키를 이용하여 직접 데이터를 암호화하기 때문에 랜덤토큰 방식처럼 중앙에서 토큰값을 관리할 필요가 없다. 때문에 분산된 환경에서 랜덤토큰 방식보다 더 쉽게 적용이 가능하다. 또한 개인정보를 암호화 서버에 저장하지 않고 SAP DB안에 암호화된 개인정보를 직접 넣기 때문에 속도가 빠르다. 또한 개인정보마다 서로 다른 암호화키를 사용하여 안전도를 더욱 강화할 수 있다는 특징이 있다. 하지만 FPE 알고리즘이 아직 인증되지 않았기 때문에 추가적인 연구가 필요하다[8].

3.6. 토큰 암호화 방식 비교

지금까지 토큰을 이용한 SAP DB암호화 방식을 간

〔표 2〕 토큰 암호화 방식 비교[9]

적용방식	랜덤토큰 방식	FPE토큰 방식
생성된 토큰	의미없는 토큰값으로 개인정보와 매핑	FPE알고리즘으로 개인정보를 토큰으로 변경
개인정보 위치	암호화 서버	원래 저장 위치
분산 환경에서의 구현 편의성	Difficult	Medium
키분배	Medium	Hard
성능	Low	Fast
토큰과 개인정보 연관성	암호화 서버에서 토큰과 매핑	알고리즘으로 암호화

단히 정리하면 아래와 같다.

랜덤토큰 방식은 개인정보를 아무런 의미없는 토큰으로 대체하고 개인정보를 별도의 서버에 암호화하여 보관하는 방식이기 때문에 보안 인프라가 갖춰진 내부망에서 적용하는 것이 적합하다. 기존의 테이블 구조를 변경하지 않기 때문에 일반 DB암호화와는 달리 기존의 인덱스를 사용하고, 사용자 권한에 따라 개인정보 조회가 필요하지 않은 경우에는 복호화 없이 값을 전달하기 때문에 기존의 성능을 유지할 수 있다. 하지만 대량의 암복호화가 발생하는 시스템에서는 다소 성능의 문제가 나타날 수 있다. SAP서버와 토큰서버간의 인터페이스가 발생하기 때문에 네트워크 통신에 따른 성능문제가 나타날 수 있다.

그에 반해 FPE방식은 암복호화 시 네트워크 통신없이 일반 DB암호화의 API방식처럼 해당 SAP서버에서 바로 개인정보를 동일한 크기의 토큰으로 암호화하기 때문에 빠른 성능을 보장한다. 하지만 각각의 SAP DB에 있는 토큰정보가 실제 개인정보이기 때문에 암호화 키 관리와 알고리즘에 대한 보안이 더 중요하다. 빠른 성능이 필요하고, 분산된 SAP 시스템을 운영하는 곳이라면 SAP에 대한 보안관리를 강화하여 FPE방식으로 SAP DB암호화 적용을 고려할만 하다.

Ⅳ. 결 론

개인정보보호기준법의 시행에 따라 ERP를 사용하는 많은 기업에서 SAP DB암호화를 적용하였고, 현재도 진행하고 있다. SAP솔루션은 기업 전체의 경영자원의 효과적인 이용을 위한 시스템이기 때문에 시스템의 성능과 안전성이 무엇보다도 중요하다. 토큰 암호화 방식은 기존의 일반 DB암호화가 가지고 있던 테이블 구조의 변경 문제에 대한 대안이 될 수 있다. 토큰 암호화 방식에 대한 더 많은 연구와 알고리즘에 대한 검증을 수행한다면 향후 토큰 방식의 암호화를 통해 SAP 시스템 뿐만 아니라 일반 DB시스템에서도 테이블 구조 변경으로 인한 문제점들을 해결할 수 있는 방안이 될 수 있을 것이다.

참고문헌

[1] 행정안전부, 개인정보의 안전성 확보조치 기준 및 해설서, 2011년 9월.
[2] http://help.sap.com/
[3] http://www.abapgogo.com
[4] http://blog.softwareinsider.org/
[5] http://211.174.114.20/?no=12099
[6] Scoping SIG, Tokenization Taskforce PCI Security Standards Council, Information Supplement: PCI DSS Tokenization Guidelines, Aug 2011
[7] Brigthwell, Michael & Smith, Using datatype preserving encryption to enhance data warehouse security, 20th National Information Systems Security Conference, NIST, 1997
[8] 보안뉴스, [기고] 토큰화 기술에 대한 보안성 고려, 2012년 5월
[9] AToS Worldline, Tokenization Format Preserving Encryption A case Study Cartes & Identification 2011, 08 Sep 2011
[10] Bellare M, Rogaway P & Spies T The FFX Mode of Operation for Format preserving Encryption. 2010.
[11] Brier E, Peyrin T & Stern J, BPS : a format Preserving Encryption Proposal. Ingenico, 2010.
[12] Ulf T Matsson, Format preserving Encryption Using Datatype preserving Encryption. 2010.

〈著者紹介〉

황 치 하 (Hwang Chi Ha)
정회원

2006년 2월 : 인하대학교 컴퓨터공학과 졸업
2006년 7월~현재 : 삼성SDS 보안컨설턴트
2012년 3월~현재 : 동국대학교 국제정보보호대학원 석사 과정
<관심분야> ISO27001, 가상화, SIEM, 암호화, 리버싱

박 준 성(Park Jun Sung)
학생회원

2008년 2월 : 방송통신대학교 컴퓨터공학과 졸업
2005년 7월~현재 : IBK시스템 근무
2012년 3월~현재 : 동국대학교 국제정보보호대학원 석사 과정
<관심분야> 네트워크분석, 리버싱, 취약점분석

최 재 우 (Choi Jae Woo)
정회원

2012년 9월 ~ 현재 : Symantec 근무
2012년 3월 ~ 현재 : 동국대학교 국제정보보호대학원 석사 과정
<관심분야> DLP, 정보보호

김 학 범 (Hak-Beom KIM)
정회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 정보보호학과 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2011년 9월~현재 : (주)지엔에스인증원 ISMS본부장
<관심분야> ISO 27001, K-ISMS, PIMS, 클라우드컴퓨팅 보안, 개인정보보호